

Nontrivial elements of Sha explained through K3 surfaces

Adam Logan and Ronald van Luijk

In this paper we present a new method to show that a principal homogeneous space of the Jacobian of a curve of genus two is nontrivial. The idea is to exhibit a Brauer-Manin obstruction to the existence of rational points on a quotient of this principal homogeneous space. In an explicit example we apply the method to show that a specific curve has infinitely many quadratic twists whose Jacobians have nontrivial Tate-Shafarevich group.

Keywords: Jacobian, Tate-Shafarevich group, Kummer surface, Brauer-Manin obstruction, genus 2 curve
MSC classification: 14H40, 11G10, 14J27-28

1 Introduction

By Faltings' Theorem every curve of genus 2 defined over a number field k has only finitely many rational points. Several methods have been developed to find all rational points of a given curve C , such as the method of Chabauty-Coleman, the Mordell-Weil sieve, and combinations of these with covering techniques. All these methods require that we know the finitely generated abelian group $J(k)$ of rational points on the Jacobian J of C , at least up to a subgroup of finite index. The torsion subgroup of $J(k)$ is generally easy to find and the problem is therefore to find the rank r of $J(k)$. The rank can be read off from the size of the group $J(k)/2J(k)$ once the torsion subgroup is known. This group fits into an exact sequence

$$0 \rightarrow J(k)/2J(k) \rightarrow \text{Sel}^{(2)}(J/k) \rightarrow \text{III}(J/k)[2] \rightarrow 0,$$

where $\text{Sel}^{(2)}(J/k)$ is the 2-Selmer group of J/k and $\text{III}(J/k)[2]$ is the 2-torsion subgroup of the Tate-Shafarevich group $\text{III}(J/k)$ of J/k . The 2-Selmer group is computable (see [18]). It is, however, not even known whether the Tate-Shafarevich group is always finite. Many papers have been devoted to exhibiting nontrivial elements of $\text{III}(J/k)$. In this paper we will follow a new method, suggested by Michael Stoll, which leads to the following result, our main theorem.

Theorem 1.0.1 *Let S be the union of $\{5\}$ with the set of primes that split completely in the field of definition of the lines of V , which is*

$$\mathbb{Q} \left(\sqrt{-1}, \sqrt{2}, \sqrt{5}, \sqrt{-3(1+\sqrt{2})}, \sqrt{6(1+\sqrt{5})} \right).$$

Then for all n which are products of elements of S , the 2-part of the Tate-Shafarevich group of the Jacobian of the curve defined by

$$y^2 = -6n(x^2 + 1)(x^2 - 2x - 1)(x^2 + x - 1)$$

is nontrivial.

Our method uses the fact that every element of $\text{Sel}^{(2)}(J/k)$ can be represented by an everywhere locally solvable 2-covering of J . A 2-covering of J is a surface X together with a morphism $\pi: X \rightarrow J$, defined over k , such that over the algebraic closure \bar{k} there exists an isomorphism $X_{\bar{k}} \cong J_{\bar{k}}$ making the following diagram

commutative.

$$\begin{array}{ccc} X_{\bar{k}} & \xrightarrow{\cong} & J_{\bar{k}} \\ & \searrow \pi & \downarrow [2] \\ & & J_{\bar{k}} \end{array}$$

The image of X in $\text{III}(J/k)$ is trivial if and only if X has a rational point. Unfortunately, the easiest way to describe X in general is as the intersection of 72 quadrics in \mathbb{P}^{15} (see [7], section 2.3 for the statement). The isomorphism in the diagram above is determined up to translation of J by a 2-torsion point. Since multiplication by -1 commutes with these translations, it induces a unique involution ι on X . Our strategy to prove that X has no rational points is to show there is a Brauer-Manin obstruction to the existence of rational points on X/ι , or rather on a minimal nonsingular model V of this quotient variety. Note that V is a twist of the Kummer surface associated to J .

The goal of this paper is twofold. In addition to proving the main theorem, we will analyze the geometry of V . By [7], chapter 16, the surface V can be embedded in \mathbb{P}^5 as the complete intersection of three quadrics. In this reference this is only done when V is a trivial twist, but we will see that it holds for any twist. In this embedding, V contains 32 lines that generically generate the Néron-Severi group of V . We will also investigate the intersection pairing among these lines and exhibit 15 pairs of elliptic fibrations, each associated to one of the nontrivial 2-torsion points of J . In section 2 we will find the fields of definition of these lines and elliptic fibrations together with explicit equations for them. Then in section 3, we will use the information we have acquired in section 2 to exhibit an explicit example for which we are able to show a Brauer-Manin obstruction. This will be the most important part of the proof of the main theorem.

We thank Michael Stoll for suggesting this project to us, Nils Bruin and Victor Flynn for helpful suggestions and explanations, William Stein for letting us use his computers, CRM in Montreal and MSRI for their hospitality and financial support, and the MAGMA group for developing their software. Also, the first author thanks the Nuffield Foundation for funding his research with a grant in their Awards to Newly Appointed Lecturers program, which supported him at CRM in the fall of 2005, and the University of Waterloo. The second author also thanks PIMS, Simon Fraser University, the University of British Columbia, and Universidad de los Andes.

2 The geometry of the surface

In this section we will investigate the geometry of the K3 surfaces that arise as the quotients of the principal homogeneous spaces under the Jacobian as described in the introduction. These K3 surfaces are twists of the Kummer surface associated to the Jacobian. In [7], sect. 16.2, it is remarked that the Kummer surface itself, i.e., the trivial twist, contains 32 lines. We will give a direct proof that all twists contain 32 lines. We will analyze the Galois action on the set of these lines. We will also describe certain elliptic fibrations, coming in pairs associated to pairs of roots of f . In the next section these will be used to find Brauer-Manin obstructions to the existence of rational points on some of these surfaces. In this section we will rarely use the fact that these K3 surfaces are twists of the Kummer surface. Given that our goal is to actually implement an algorithm, we will keep everything very explicit, including our proofs. We will, however, refer to [7] at times in order not to lose the context our work should be seen in.

2.1 The surface

Let k be a field and W a vector space over k of dimension $r \geq 1$. We let $\mathbb{P}(W)$ denote the projective space $(W - \{0\})/k^*$ associated to W . The homogeneous coordinate ring of $\mathbb{P}(W)$ is the symmetric algebra $S(\widehat{W}) = \bigoplus_{n \geq 0} S^n(\widehat{W})$, where $\widehat{W} = \text{Hom}_k(W, k)$ is the dual of W . Let (x_1, \dots, x_r) be a basis of \widehat{W} . This basis yields an isomorphism $\mathbb{P}(W) \rightarrow \mathbb{P}_k^{r-1}$ that sends the element $w \in W$ to $[x_1(w) : \dots : x_r(w)]$. Thus the x_i determine a coordinate system on $\mathbb{P}(W)$. The symmetric algebra $S(\widehat{W})$ is isomorphic to the polynomial ring $k[x_1, \dots, x_r]$.

Let $f \in k[X]$ be a separable polynomial of degree 6, and set $A_f = k[X]/f$. Consider $\delta \in A_f^*$ and set

$$\mathcal{V}_{f,\delta} = \{q \in A_f : \exists c_0, c_1, c_2 \text{ such that } \delta q^2 = c_2 X^2 + c_1 X + c_0\}.$$

Let $V_{f,\delta}$ denote the subset of $\mathbb{P}(A_f)$ corresponding to $\mathcal{V}_{f,\delta}$. For any $c \in k^*$ we obviously have $A_{cf} = A_f$, $\mathcal{V}_{cf,\delta} = \mathcal{V}_{f,\delta}$, and $V_{cf,\delta} = V_{f,\delta}$. We will often leave any subscript out of the notation that is clear from the context. Let (a_0, \dots, a_5) be the canonical basis of \hat{A} associated to the basis $(1, X, \dots, X^5)$ of A , so that any $q \in A$ can be written as $q = \sum_{i=0}^5 a_i(q)X^i$. As above the a_i determine a coordinate system on $\mathbb{P}(A)$. Writing out δq^2 , we see that there are quadratic forms C_0, \dots, C_5 in the homogeneous coordinate ring $S(\hat{A})$ of $\mathbb{P}(A)$, depending on f and δ , such that $a_i(\delta q^2) = C_i(q)$ for any $q \in A$. We have $q \in \mathcal{V}$ if and only if we have $C_i(q) = 0$ for $3 \leq i \leq 5$. This implies that V is an algebraic set in $\mathbb{P}(A)$, defined over k by the three quadrics C_3, C_4 , and C_5 . We will express the C_i in a new coordinate system, inspired by [7], Chapter 16.

For any field extension k' of k we write $A_{k'} = A \otimes_k k'$, viewed as a vector space over k' , so that we have $\mathbb{P}(A_{k'}) \cong \mathbb{P}(A)_{k'}$. We write \bar{A} and \bar{V} for $A_{\bar{k}}$ and $V_{\bar{k}}$ respectively, where \bar{k} is a fixed algebraic closure of k . Let Ω denote the set of roots of f in \bar{k} . Then $l = k(\Omega)$ is the splitting field of f . For $\omega \in \Omega$ we let φ_ω denote the l -algebra homomorphism $A_l \rightarrow l$ given by $X \mapsto \omega$. The φ_ω form a basis of \hat{A}_l and therefore induce a coordinate system on $\mathbb{P}(A_l)$.

Remark 2.1.1 Let $(P_\omega)_\omega$ be the canonical basis of A_l associated to the basis $(\varphi_\omega)_\omega$ of \hat{A}_l . Then for each $q \in A_l$ we have

$$C_i(q) = a_i(\delta q^2) = a_i\left(\sum_\omega \varphi_\omega(\delta q^2)P_\omega\right) = \sum_\omega a_i(P_\omega)\varphi_\omega(\delta)\varphi_\omega(q)^2,$$

which implies $C_i = \sum_\omega a_i(P_\omega)\delta_\omega\varphi_\omega^2$, with $\delta_\omega = \varphi_\omega(\delta)$. Note that we have $\varphi_\omega = \sum_{i=0}^5 \omega^i a_i$, so we can also write the C_i in terms of the coordinates a_i . We can make the constants $a_i(P_\omega)$ explicit by setting $P'_\omega = \prod_{\theta \in \Omega \setminus \{\omega\}} (X - \theta)$. Then P_ω equals the Legendre polynomial $P'_\omega(\omega)^{-1}P'_\omega$.

For all $\omega \in \Omega$ we set $\lambda_\omega = \varphi_\omega(P'_\omega) = P'_\omega(\omega)$ with P' as in Remark 2.1.1. For $j = 0, 1, 2$, set

$$Q_j = \sum_\omega \omega^j \lambda_\omega^{-1} \delta_\omega \varphi_\omega^2.$$

Convention 1 From now on we will assume that the characteristic of k is different from 2.

Proposition 2.1.2 *The algebraic set $V_{f,\delta}$ is a smooth, geometrically integral complete intersection of the three quadrics Q_0, Q_1 , and Q_2 . It is a K3 surface of degree 8.*

Proof. Suppose $f = \sum_{i=0}^6 f_i X^i$. The set V is defined by the quadrics C_3, C_4, C_5 , so it is also defined by

$$Q'_0 = C_5, \quad Q'_1 = C_4 - f_5 f_6^{-1} C_5, \quad \text{and} \quad Q'_2 = C_3 - f_5 f_6^{-1} C_4 + (f_5^2 f_6^{-2} - f_4 f_6^{-1}) C_5.$$

From the equations $-f_5 f_6^{-1} = \sum_\omega \omega$ and $f_4 f_6^{-1} = \sum_{\psi \neq \omega} \psi \omega$ we find $Q'_i = Q_i$ for $i = 0, 1, 2$. One checks that the quadrics define a smooth complete intersection. Every smooth complete intersection of three quadrics in \mathbb{P}^5 is a K3 surface of degree 8. \square

Remark 2.1.3 The statement that V is a K3 surface also follows from the fact that V is the twist by δ of the desingularized Kummer surface associated to the Jacobian of the curve given by $y^2 = f$; see [7], Chapter 16.

Corollary 2.1.4 *The Néron-Severi group $\text{NS}(V)$ of V is free, finitely generated, isomorphic to $\text{Pic } V$, and it has a lattice structure induced by the intersection pairing.*

Proof. There are injections $\text{Pic } V \hookrightarrow \text{Pic } \bar{V}$ and $\text{Pic}^0 V \hookrightarrow \text{Pic}^0 \bar{V}$. As V is a complete intersection by Proposition 2.1.2, we find from [8], Thm. 1.8, that $\text{Pic}^0 \bar{V} = 0$, so $\text{NS}(V) = \text{Pic } V$. The Néron-Severi group of any projective variety is finitely generated, see [9], exc. V.1.7. Also by [8], Thm. 1.8, we find that $\text{Pic } \bar{V}$ is torsion-free, so it is free. In general the intersection pairing induces a lattice structure on the Néron-Severi group modulo torsion (see [10]), which in this case is isomorphic to $\text{Pic } V$.

This theorem also follows from the fact that V is a K3 surface, as shown for characteristic 0 in Prop. VIII.3.2 and on page 120 of [1], and for positive characteristic in Theorem 5 of [2]. \square

Remark 2.1.5 Consider the net of quadrics $pQ_0 + qQ_1 + rQ_2$ vanishing on V . The curve C in $\mathbb{P}^2(p, q, r)$ corresponding to singular quadrics is given by the equation $\det(pM_0 + qM_1 + rM_2) = 0$ of degree 6, where M_i is the symmetric matrix corresponding to the quadratic form Q_i . For any $\omega \in \Omega$ the quadric hypersurface corresponding to any point on the line $p + \omega q + \omega^2 r = 0$ is singular at the point in $\mathbb{P}(A_l)$ given by $\varphi_\theta = 0$ for all $\theta \neq \omega$. This implies that C consists of 6 lines. The 15 intersection points are parametrized by pairs $(\omega, \psi) \in \Omega^2$ with $\omega \neq \psi$. The corresponding quadrics are given by $Q_{\omega\psi} = \omega\psi Q_0 - (\omega + \psi)Q_1 + Q_2$. The hypersurface given by $Q_{\omega\psi}$ is singular at every point on the line $m_{\omega\psi}$ given by $\varphi_\theta = 0$ for $\theta \neq \omega, \psi$. This hypersurface is a cone over a quadric $D_{\omega\psi}$ in the \mathbb{P}^3 obtained by projecting $\mathbb{P}(A_l)$ away from $m_{\omega\psi}$, and therefore contains two families of linear three-spaces. Each family cuts out a family of curves on V , given by the two quadrics Q_0, Q_1 in these three-spaces. This yields two elliptic fibrations of V , both defined over a quadratic extension of $k(\omega\psi, \omega + \psi)$. We will see later which extension this is. Note that the projection from $m_{\omega\psi}$ induces a 4-to-1 map from V to $D_{\omega\psi}$. The elliptic fibrations factor through this map. Since $D_{\omega\psi}$ satisfies the Hasse principle this map may be used to obtain information about the arithmetic of V .

Let k' be any field extension of k . For every $z \in A_{k'}^*$, let $[z]$ denote the automorphism of $\mathbb{P}(A_{k'})$ induced by multiplication by z . Note that $[z]$ maps V_δ isomorphically to $V_{\delta z^{-2}}$, so if δ is a square in $A_{k'}^*$, then V_δ is isomorphic to V_1 over k' . For any commutative ring R let $\mu(R)$ denote the kernel of the endomorphism $x \mapsto x^2$ of R^* . The scheme $\text{Spec } A[t]/(t^2 - 1)$ represents the functor from the category of A -algebras to the category of groups that sends R to $\mu(R)$ in the sense that the elements of $\mu(R)$ are parametrized by the maps from $\text{Spec } R$ to $\text{Spec } A[t]/(t^2 - 1)$ that respect the map to $\text{Spec } A$. Such a map corresponds to the image of t under the associated homomorphism $A[t]/(t^2 - 1) \rightarrow R$. Let μ_A be the Weil restriction of this scheme associated to the extension A/k . Then μ_A is a k -scheme representing the functor that sends a field extension l of k to $\mu(A_l)$. Let $\tilde{\mu}$ be the quotient of μ_A by the automorphism that is induced by $t \mapsto -t$ on $\text{Spec } A[t]/(t^2 - 1)$. Then for all field extensions l of k we have $\tilde{\mu}(l) = (\mu(A_l)/\langle -1 \rangle)^{G_l}$, where G_l is the absolute Galois group of l .

Lemma 2.1.6 *The homomorphism $A_{k'}^* \rightarrow \text{Aut}_{k'} \mathbb{P}(A_{k'})$ that sends z to $[z]$ has kernel k'^* . It induces an injective homomorphism $\tilde{\mu}(k') \rightarrow \text{Aut}_{k'} V_{k'}$.*

Proof. Note that for $z \in \mu(A_{k'})'$ the automorphisms $[z]$ and $[-z]$ are equal, so the homomorphism $\tilde{\mu}(k') \rightarrow \text{Aut}_{\bar{k}} V_{\bar{k}}$ is well defined and has image in $\text{Aut}_{k'} V_{k'}$. We may therefore assume that k' is algebraically closed, so that $\tilde{\mu}(k') = \mu(A_{k'})/\langle -1 \rangle$. Let ρ denote the homomorphism $z \mapsto [z]$ in question. If $\rho(z)$ is the identity, then we have $z \cdot 1 = 1$ in $(A_{k'} - \{0\})/k'^*$, which implies $z \in k'^*$. Set $H_V = \{\tau \in \text{Aut}_{k'} \mathbb{P}(A_{k'}) : \tau(V) = V\}$. Since $[z]$ maps V_δ to $V_{\delta z^{-2}}$, the restriction ρ_μ of ρ to $\mu(A_{k'})$ factors through H_V . Because V is not contained in a hyperplane, the map $H^0(\mathbb{P}^5, \mathcal{O}_{\mathbb{P}^5}(1)) \rightarrow H^0(V, \mathcal{O}_V(1))$ is injective. As every element in $\text{Aut}_{k'} \mathbb{P}_{k'}^5$ is determined by its action on $H^0(\mathbb{P}^5, \mathcal{O}_{\mathbb{P}^5}(1))$, this implies that the restriction map $r: H_V \rightarrow \text{Aut}_{k'} V_{k'}$ is injective. Hence, the composition $r \circ \rho_\mu: \mu(A_{k'}) \rightarrow \text{Aut}_{k'} V_{k'}$ has kernel $\ker \rho_\mu = \mu(A_{k'}) \cap k'^* = \{\pm 1\}$ and therefore induces the injective homomorphism already mentioned. \square

For any $\zeta \in \mu(A_{k'})$ we write $\tilde{\zeta}$ for the image of ζ in $\tilde{\mu}(k')$, and $[\zeta]$ or $[\tilde{\zeta}]$ for the induced action by multiplication on $\mathbb{P}(A_{k'})$ and $V_{k'}$. Let T be the Weil restriction of the scheme $\text{Spec } A[t]/(t^2 - \delta)$ associated to the extension A/k and let \tilde{T} be the k -scheme that is the quotient of T by the automorphism induced by $t \mapsto -t$ on

$\text{Spec } A[t]/(t^2 - \delta)$. As for μ_A and $\tilde{\mu}$ above, we can make the identifications

$$T(l) = \{\xi \in A_l : \xi^2 = \delta\}, \quad \text{and} \quad \tilde{T}(l) = (\{\xi \in A_l : \xi^2 = \delta\} / \langle [-1] \rangle)^{G_l}.$$

Clearly T is a k -torsor under μ_A , with the transitive free action of $\mu_A(k') = \mu(A_{k'})$ on $T(k')$ given by multiplication in $A_{k'}$. Similarly, \tilde{T} is a k -torsor under $\tilde{\mu}$.

For any $\xi \in T(k')$ the 2-dimensional subspace

$$\mathcal{L}_\xi = \{\xi^{-1}(sX + t) : s, t \in k'\}$$

of $A_{k'}$ corresponds to a line in $\mathbb{P}(A_{k'})$, defined over k' , which is contained in $V_{k'}$ and which we will denote by L_ξ . Since $L_\xi = L_{-\xi}$, this implies that to each $\tilde{\xi} \in \tilde{T}(k')$ we can associate a unique line $L_{\tilde{\xi}}$, namely $L_{\tilde{\xi}} = L_\xi$, where $\xi \in T(\bar{k}')$ is a lift of $\tilde{\xi}$. Let $\Lambda(k')$ denote the set of all lines $L_{\tilde{\xi}}$ corresponding to some $\tilde{\xi} \in \tilde{T}(k')$. Note that for any $z \in \mu(A_{\bar{k}'})$ the automorphism $[z]$ maps L_ξ to $L_{\xi z^{-1}}$. This induces an action of $\tilde{\mu}(k')$ on $\Lambda(k')$.

Lemma 2.1.7 *The action of $\tilde{\mu}(k')$ on $\Lambda(k')$ is transitive and free.*

Proof. Transitivity follows from the fact that the action of $\mu(A_{\bar{k}'})$ on $T(\bar{k}')$ is transitive and the map $\tilde{T}(k') \rightarrow \Lambda(k')$ sending $\tilde{\xi}$ to $L_{\tilde{\xi}}$ is surjective and respects the action of $\mu(A_{k'})$. To show that the action is free, we may assume that k' is algebraically closed. Suppose that for $\tilde{\zeta} \in \tilde{\mu}(k')$ we have $\tilde{\zeta}L_\xi = L_\xi$ and let $\zeta \in \mu(A_{k'})$ be a lift of $\tilde{\zeta}$. Then multiplication by ζ sends the subspace \mathcal{L}_ξ to itself, so it also sends the subspace $W = \{sX + t : s, t \in k'\}$ to itself. In particular this implies that there are $s, t \in k'$ such that $\zeta \cdot 1 = sX + t$. From the fact that $\zeta \cdot X \in W$ we then find $s = 0$, so $\zeta = t$ is in $\mu(A_{k'}) \cap k' = \{\pm 1\}$, which means $\tilde{\zeta} = 1$. We conclude that the action of $\tilde{\mu}(k')$ on $\Lambda(k')$ is free. \square

Lemma 2.1.8 *The map $T(\bar{k}') \rightarrow \Lambda(\bar{k}')$ that sends ξ to L_ξ induces a bijection $\tilde{T}(k') \rightarrow \Lambda(k')$ that respects the action of $\tilde{\mu}(k')$ and $G(\bar{k}/k)$.*

Proof. It is obvious that we obtain a surjective map $\tilde{T}(k') \rightarrow \Lambda(k')$ that respects the action of $\tilde{\mu}(k')$ and $G(\bar{k}/k)$. Injectivity then follows from the fact that $\tilde{\mu}(k')$ acts transitively and freely on both $\tilde{T}(k')$ and $\Lambda(k')$, as we saw in Lemma 2.1.7. \square

Remark 2.1.9 Lemmas 2.1.7 and 2.1.8 combined say that $\tilde{T}(\bar{k})$ and $\Lambda(\bar{k})$ are isomorphic over k as k -torsors under $\tilde{\mu}(\bar{k})$.

Convention 2 For the rest of this section we will suppose that l is contained in k' .

By the Chinese Remainder Theorem, the map

$$\varphi_{k'}: A_{k'} \rightarrow \bigoplus_{\omega \in \Omega} k'$$

induced by the φ_ω is an isomorphism, defined over l . Note that the induced Galois action on $\bigoplus_\omega k'$ is given by acting on both the indices and the coefficients in k' . In other words, for $\sigma \in G(\bar{k}/k)$ we have

$$\sigma((c_\omega)_{\omega \in \Omega}) = (\sigma c_{\sigma^{-1}\omega})_{\omega \in \Omega}.$$

It follows that $\mu(A_{k'})$ and $\tilde{\mu}(k')$ are isomorphic to $\bigoplus_\omega \{\pm 1\}$ and $(\bigoplus_\omega \{\pm 1\})/\{\pm 1\}$ respectively.

Lemma 2.1.10 *Either the set $\Lambda(k')$ is empty, or it contains exactly 32 lines.*

Proof. Since $\tilde{\mu}(k')$ has exactly 32 elements, this follows from Lemma 2.1.7. \square

For $I \subset \Omega$ let ζ_I denote the unique element in $\mu(A_{k'})$ with $\varphi_\omega(\zeta_I) = -1$ for $\omega \in I$ and $\varphi_\omega(\zeta_I) = 1$ for $\omega \notin I$. Note that we have $\tilde{\zeta}_I = \tilde{\zeta}_{\Omega \setminus I}$. We will also denote this element by $\tilde{\zeta}_\pi$, where π is the partition $\{I, \Omega \setminus I\}$ of Ω . The map from the set $\mathcal{P}(\Omega)$ of all subsets of Ω to $\mu(A_{k'})$ that sends I to ζ_I is a bijection. It induces a bijection from the set Π of partitions of Ω into two sets to $\tilde{\mu}(k')$, sending π to $\tilde{\zeta}_\pi$. The inverse $\pi: \tilde{\mu}(k') \rightarrow \Pi$ of the latter bijection is given by

$$\pi(\tilde{\zeta}) = \{\{\omega : \varphi_\omega(\zeta) = 1\}, \{\omega : \varphi_\omega(\zeta) = -1\}\},$$

where $\zeta \in \mu(A_{k'})$ is a lift of $\tilde{\zeta}$. For any $\pi = \{I, J\} \in \Pi$ the automorphism $[\tilde{\zeta}_\pi] = [\zeta_I]$ is defined over the fixed field of the group $\{g \in G(k/k) : {}^g\pi = \pi\}$. Note that $[\zeta_I]$ acts on $\mathbb{P}(A_I)$ by sending the coordinate φ_ω to $\pm\varphi_\omega$, where the sign is negative if and only if we have $\omega \in I$.

For any $\omega \in \Omega$ and $\xi \in T(k')$ we let $P_{\xi, \omega}$ denote the point on the line L_ξ corresponding to the set

$$\{\xi^{-1}s(X - \omega) : s \in k'\} \subset A_{k'}.$$

For any $z \in \mu(A_{k'})$ the map $[z]$ sends $P_{\xi, \omega}$ to $P_{\xi z^{-1}, \omega}$. The notation distinguishes the points $P_{\xi, \omega}$, indexed by two subscripts, from the polynomials P_ω from Remark 2.1.1, which are indexed by only one.

Proposition 2.1.11 *For all $\omega \in \Omega$ and all $\xi \in T(k')$ we have $\zeta_\omega P_{\xi, \omega} = P_{\xi, \omega}$. Two lines $L, L' \in \Lambda(k')$ intersect if and only if there exists an $\omega \in \Omega$ such that $\zeta_\omega L = L'$, in which case the intersection point is $P_{\xi, \omega} = P_{\xi', \omega}$, where $\xi, \xi' \in T(k')$ are such that $L = L_\xi$ and $L' = L_{\xi'}$.*

Proof. One easily checks $\varphi((\zeta_\omega - 1)(X - \omega)) = 0$, so we have $X - \omega = \zeta_\omega(X - \omega)$ for all $\omega \in \Omega$. This implies that for all $\xi \in T(k')$ we have $\zeta_\omega P_{\xi, \omega} = P_{\xi \zeta_\omega^{-1}, \omega} = P_{\xi, \omega}$, which proves the first statement. Let $\xi, \xi' \in T(k')$ be such that $L = L_\xi$ and $L' = L_{\xi'}$. Suppose there is an $\omega \in \Omega$ such that $\zeta_\omega L = L'$. Then L and L' both go through the point $P_{\xi, \omega} = \zeta_\omega P_{\xi', \omega}$, so they intersect.

Conversely, suppose L and L' intersect. Then the subspaces \mathcal{L}_ξ and $\mathcal{L}_{\xi'}$ have a nonzero intersection, so we can choose $s, t, s', t' \in k'$ such that $\xi^{-1}(sX + t) = \xi'^{-1}(s'X + t') \neq 0$. Applying φ_ω we find $\varphi_\omega(\zeta)(s\omega + t) = s'\omega + t'$ for all $\omega \in \Omega$, with $\zeta = \xi^{-1}\xi' \in \mu(A_{k'})$. After replacing ξ' by $-\xi'$ if necessary, we may assume that there are at least three $\omega \in \Omega$ with $\varphi_\omega(\zeta) = 1$. Then the equation $sx + t = s'x + t'$ has at least three solutions in x , which implies $s' = s$ and $t' = t$. From $L \neq L'$ we deduce $\zeta \neq 1$, so there is an ω with $\varphi_\omega(\zeta) \neq 1$. The equation $\varphi_\omega(\zeta)(s\omega + t) = s'\omega + t' = s\omega + t$ then yields $s\omega + t = 0$. Since the equation $sx + t = 0$ has at most one solution in x , this shows $\zeta = \zeta_\omega$ and $\zeta_\omega L = L'$. \square

Corollary 2.1.12 *For any line $L \in \Lambda(k')$ and any elements $\tilde{\zeta}, \tilde{\zeta}' \in \tilde{\mu}(k')$ the lines $\tilde{\zeta}L$ and $\tilde{\zeta}'L$ intersect if and only if we have $\tilde{\zeta} \cdot \tilde{\zeta}' = \tilde{\zeta}_\omega$ for some $\omega \in \Omega$.*

Proof. By Lemma 2.1.7 the element $\tilde{\zeta}'' = \tilde{\zeta} \cdot \tilde{\zeta}' = \tilde{\zeta}^{-1} \cdot \tilde{\zeta}'$ is the unique element in $\tilde{\mu}(k')$ for which we have $\tilde{\zeta}'' \cdot \tilde{\zeta}L = \tilde{\zeta}'L$. By Proposition 2.1.11 the lines intersect if and only if we have $\tilde{\zeta}'' = \tilde{\zeta}_\omega$ for some $\omega \in \Omega$. \square

Put $\bar{A} = A_{\bar{k}}$, $\bar{V} = V_{\bar{k}}$, and $\bar{\Lambda} = \Lambda(\bar{k})$. For any $L, L' \in \bar{\Lambda}$ we say that L and L' have the same or opposite parity if for the unique $\tilde{\zeta} \in \tilde{\mu}(\bar{k})$ with $\tilde{\zeta}L = L'$, the number of elements of the sets in the partition $\pi(\tilde{\zeta})$ is even or odd respectively. For any $\omega, \psi \in \Omega$, let $\Phi_{\omega\psi}$ denote the subgroup of $\tilde{\mu}(\bar{k})$ generated by $\tilde{\zeta}_\omega$ and $\tilde{\zeta}_\psi$.

Lemma 2.1.13 *Let $L, L' \in \bar{\Lambda}$ be different lines of the same parity. Then L and L' do not intersect and there are exactly two lines M and M' of the opposite parity that intersect both L and L' . There are $\omega, \psi \in \Omega$ such that the set $\{L, L', M, M'\}$ is an orbit of $\bar{\Lambda}$ under the action of $\Phi_{\omega\psi}$.*

Proof. Let $I \subset \Omega$ be such that $\zeta_I L = L'$. Then $\#I$ is even, so L and L' do not intersect by Corollary 2.1.12. After replacing I by $\Omega \setminus I$ if necessary, there are $\omega, \psi \in \Omega$, such that $I = \{\omega, \psi\}$. From Corollary 2.1.12 we deduce that the only lines that intersect both L and L' are $M = \zeta_\omega L$ and $M' = \zeta_\psi L$. Indeed the set $\{L, L', M, M'\}$ is an orbit under $\Phi_{\omega\psi}$. \square

Remark 2.1.14 Remembering that \bar{V} is a twist of the Kummer surface associated to the Jacobian J of the curve given by $y^2 = f(x)$, we note that the lines of one parity correspond to the 16 blow-ups of the nodes on the singular surface $J/\langle -1 \rangle$. The lines of the other parity correspond to the tropes, see [7], Sect. 3.7. The intersection numbers among these lines are well known.

Definition 2.1.15 A 4-gon is a set $\{L, L', M, M'\}$ of four lines, such that L and L' intersect both M and M' .

By Lemma 2.1.13 any two lines of the same parity determine a unique 4-gon. All 4-gons arise in this way, because if the lines L and L' both intersect a line M , then by Lemma 2.1.13 both L and L' are of the opposite parity than M , so L and L' have the same parity.

Lemma 2.1.16 Let $\omega, \psi \in \Omega$ and any $I, J \subset \Omega$ be such that the lines $\zeta_I L$ and $\zeta_J L$ are not in the same orbit under $\Phi_{\omega\psi}$. Then the cardinalities of the sets $I \cap (\Omega \setminus \{\omega, \psi\})$ and $J \cap (\Omega \setminus \{\omega, \psi\})$ have different parity if and only if the line $\zeta_I L$ intersects some line in the orbit under $\Phi_{\omega\psi}$ of the line $\zeta_J L$ in which case it intersects exactly one line in this orbit.

Proof. Suppose that the cardinalities of the sets $I \cap (\Omega \setminus \{\omega, \psi\})$ and $J \cap (\Omega \setminus \{\omega, \psi\})$ have the same parity and that they are not equal. Let $\pi = \{\pi_1, \pi_2\} \in \Pi$ be such that $\zeta_\pi = \tilde{\zeta}_I \tilde{\zeta}_J$. Then $\zeta_I L$ and $\zeta_J L$ are in the same orbit under $\Phi_{\omega\psi}$ if and only if we have $\pi_i \subset \{\omega, \psi\}$ for $i = 1$ or $i = 2$. We conclude $\pi_i \not\subset \{\omega, \psi\}$ for $i = 1, 2$. Suppose that $I \cap (\Omega \setminus \{\omega, \psi\})$ and $J \cap (\Omega \setminus \{\omega, \psi\})$ have the same parity. Then $\pi_i \cap (\Omega \setminus \{\omega, \psi\}) \neq \emptyset$ has even parity for $i = 1$ and $i = 2$. It follows that for each $\tilde{\zeta} \in \Phi_{\omega\psi}$ the sets in the partition $\pi(\zeta \zeta_I \zeta_J) = \pi(\zeta \zeta_\pi)$ contain exactly 2 elements of $\Omega \setminus \{\omega, \psi\}$, so $\zeta_I L$ does not intersect any of the lines $\tilde{\zeta} \zeta_J L$ in the orbit of $\zeta_J L$ by Corollary 2.1.12.

Conversely, suppose that $I \cap (\Omega \setminus \{\omega, \psi\})$ and $J \cap (\Omega \setminus \{\omega, \psi\})$ have different parity. Then we have $\pi = \{K \cup \{\theta\}, \Omega \setminus (\{\theta\} \cup K)\}$ for some $\theta \in \Omega \setminus \{\omega, \psi\}$ and $K \subset \{\omega, \psi\}$. Then by Corollary 2.1.12 the line $\zeta_I L$ intersects exactly one line in the orbit of $\zeta_J L$, namely $\tilde{\zeta}_K \tilde{\zeta}_J L$. \square

Lemma 2.1.17 Let F_1 be a 4-gon. Then there are exactly 12 lines in Λ that do not intersect any line in F_1 . The set of these 12 lines can be partitioned into three 4-gons F_2, F_3, F_4 and no other subset of this set is a 4-gon. The set of the remaining 16 lines can be partitioned into four 4-gons G_1, G_2, G_3, G_4 in such a way that, for every $i, j \in \{1, 2, 3, 4\}$, each line in F_i intersects exactly one of the lines in G_j and each line in G_i intersects exactly one of the lines in F_j . For any different $i, j \in \{1, 2, 3, 4\}$, no line in F_i intersects a line in F_j and no line in G_i intersects a line in G_j . There are $\omega, \psi \in \Omega$ such that the F_i and G_i are the orbits of Λ under the action of $\Phi_{\omega\psi}$. If L is a line in F_1 , then for $i \in \{2, 3, 4\}$ there are $\theta, \theta' \in \Omega \setminus \{\omega, \psi\}$ such that F_i is the orbit of $L_{\theta\theta'}$, and for $j \in \{1, 2, 3, 4\}$ there is a $\theta \in \Omega \setminus \{\omega, \psi\}$ such that G_j is the orbit of L_θ .

Proof. Let $\omega, \psi \in \Omega$ be such that F_1 is an orbit under $\Phi_{\omega\psi}$, and let L denote some line in F_1 . For any $\theta, \theta' \in \Omega \setminus \{\omega, \psi\}$ the lines $\zeta_{\theta\theta'} L$ and $\zeta_{\omega\theta\theta'} L$ do not intersect any line in F_1 by Lemma 2.1.16. This gives 12 lines and one checks that the only three 4-gons contained in the set of these 12 lines are of the form

$$\{\zeta_{\theta_1\theta_2} L, \zeta_{\theta_3\theta_4} L, \zeta_{\omega\theta_1\theta_2} L, \zeta_{\omega\theta_3\theta_4} L\},$$

for some permutation $(\theta_i)_i$ of the elements in $\Omega \setminus \{\omega, \psi\}$. From the equalities $\zeta_{\theta_3\theta_4} L = \zeta_{\omega\psi\theta_1\theta_2} L$ and $\zeta_{\omega\theta_3\theta_4} L = \zeta_{\psi\theta_1\theta_2} L$ we deduce that these 4-gons are also orbits under $\Phi_{\omega\psi}$, each containing an element $L_{\theta\theta'}$ for some $\theta, \theta' \in \Omega \setminus \{\omega, \psi\}$. The remaining 16 lines do intersect a line in F_1 by Lemma 2.1.16 and the only four 4-gons contained in the set of these 16 lines are of the form

$$\{\zeta_\theta L, \zeta_{\omega\theta} L, \zeta_{\psi\theta} L, \zeta_{\omega\psi\theta} L\},$$

for some $\theta \in \Omega \setminus \{\omega, \psi\}$. Clearly these 4-gons are orbits under $\Phi_{\omega\psi}$ as well. The remaining statements follow from Lemma 2.1.16. \square

Definition 2.1.18 An exhibit is a quadruple $\mathcal{S} = \{S_1, S_2, S_3, S_4\}$ of 4-gons such that the S_i are pairwise disjoint and no line in S_i intersects a line in S_j for $i \neq j$. A gallery is an unordered pair $\{S_1, S_2\}$ of exhibits, such that $\bigcup_{S \in \mathcal{S}_1}$ and $\bigcup_{S \in \mathcal{S}_2}$ are disjoint. For any gallery $\{S_1, S_2\}$ we say that S_2 is the complementary exhibit of S_1 .

Remark 2.1.19 Lemma 2.1.17 says that each 4-gon is contained in a unique exhibit, which is contained in a unique gallery. It also implies that the set of galleries is in bijection with the set of 15 pairs of different elements in Ω . Figure 1 displays a gallery and the intersections among all the 32 lines in Λ . In Figure 1 we use the notation I for $\zeta_I L$ for some fixed line L . The elements of Ω are denoted by $\omega, \psi, 1, 2, 3, 4$. The two exhibits are made up by the 4-gons on the bottom and the left of the figure respectively.

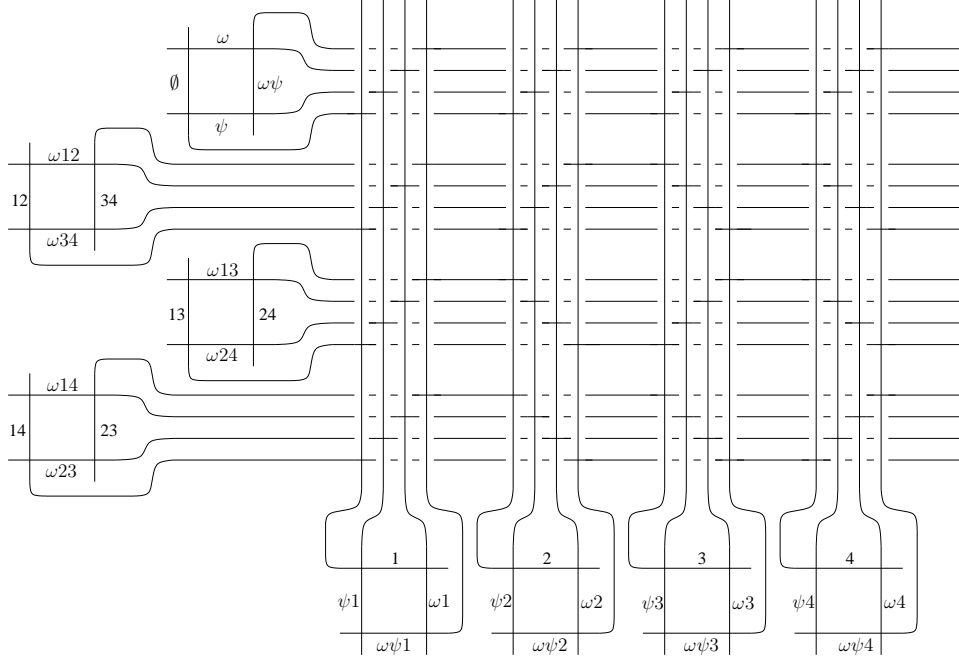


Figure 1: the intersections among the 32 lines in Λ

Lemma 2.1.20 For each smooth curve C of genus g on a K3 surface, we have $C^2 = 2g - 2$.

Proof. The adjunction formula gives $C \cdot (C + K) = 2g - 2$, where K is the canonical divisor of the surface. The lemma follows from the fact that the canonical divisor of a K3 surface is trivial. \square

Proposition 2.1.21 The elements of Λ generate a sublattice of the Néron-Severi group $\text{NS}(\bar{V})$ of rank 17 and discriminant 64.

Proof. Lemma 2.1.20 implies that $L^2 = -2$ for all $L \in \Lambda$. From Corollary 2.1.12 we can deduce all other intersection numbers among elements of Λ . This gives a 32×32 Gram matrix of intersection numbers that has rank 17. The matrix also allows us to pick a basis of this sublattice. The Gram matrix with respect to such a basis turns out to have determinant 64. \square

Proposition 2.1.22 The rank of the Néron-Severi group $\text{NS}(\bar{V})$ equals $16 + \text{rk NS}(J)$, where J is the Jacobian of the curve given by $y^2 = f(x)$.

Proof. The surface \bar{V} is isomorphic to the desingularized Kummer surface associated to J by [7], Chapter 16. The statement therefore follows from [17], Prop. 1. \square

Proposition 2.1.23 *Generically the lines in Λ generate a lattice of finite index in the Néron-Severi group $\text{NS}(\bar{V})$.*

Proof. Let J be as in Proposition 2.1.22. Generically we have $\text{rk NS}(J) = 1$, so $\text{rk NS}(\bar{V}) = 17$. By Proposition 2.1.21 the elements of Λ generate a lattice of rank 17 as well, so this lattice has finite index in $\text{NS}(\bar{V})$. \square

In fact the finite index in Proposition 2.1.23 is equal to 1 as we will see in Proposition 2.1.30. The reason for stating that result separately is that one can compute the rank of the Néron-Severi group in explicit cases using methods from [19] and [20].

For any 4-gon S let D_S denote the divisor that is the sum of the lines in S .

Lemma 2.1.24 *Let S and S' be two 4-gons in complementary exhibits. Then the image of $D_S + D_{S'}$ in $\text{Pic } \bar{V}$ is the class of hyperplane sections.*

Proof. Let L be a line in S and let $\omega, \psi \in \Omega$ be such that S is the orbit of L under $\Phi_{\omega\psi}$. By Lemma 2.1.17, the 4-gon S' is also an orbit under $\Phi_{\omega\psi}$. It follows from Lemma 2.1.16 that there is a $\theta \in \Omega \setminus \{\omega, \psi\}$ such that S' is the orbit of $\zeta_\theta L$. We deduce

$$D_S + D_{S'} = L + \zeta_\omega L + \zeta_\psi L + \zeta_{\psi\omega} L + \zeta_\theta L + \zeta_{\theta\omega} L + \zeta_{\theta\psi} L + \zeta_{\theta\psi\omega} L.$$

One checks that for each $L' \in \Lambda$ we have $(D_S + D_{S'}) \cdot L' = 1$. For a hyperplane section H we also have $H \cdot L' = 1$ for all $L' \in \Lambda$. Since the intersection pairing on $\text{Pic } \bar{V}$ is nondegenerate and the lines generically generate a lattice of finite index in $\text{Pic } \bar{V}$ by Proposition 2.1.23, we find that generically $D_S + D_{S'}$ is a hyperplane section. By specializing the transcendentals, this implies that $D_S + D_{S'}$ is always a hyperplane section. \square

Lemma 2.1.25 *Let S and S' be two 4-gons in the same exhibit. Then D_S and $D_{S'}$ are linearly equivalent.*

Proof. Let S'' be any 4-gon in the complementary exhibit, and let H denote a hyperplane section. Then by Lemma 2.1.24 both D_S and $D_{S'}$ are linearly equivalent with $H - D_{S''}$. \square

Proposition 2.1.26 *Let X be a K3 surface over a field and F a reduced and connected curve on X that satisfies $F^2 = 0$. Suppose further that the linear system $|F|$ does not have a base curve. Then there is an elliptic fibration $X \rightarrow \mathbb{P}^1$ whose fibers are the elements of $|F|$. Up to an automorphism of \mathbb{P}^1 this fibration is unique.*

Proof. By the adjunction formula we have $F \cdot (F + K_X) = 2p_a - 2$, where p_a is the arithmetic genus of F , but $F^2 = 0$ and $K_X = 0$, so $p_a = 1$. By the Riemann-Roch theorem for surfaces ([9], thm. V.1.6), we have $h^0(\mathcal{O}_X(-F)) - h^1(\mathcal{O}_X(-F)) + h^0(\mathcal{O}_X(K_X + F)) = 1/2(F \cdot (F - K_X)) + 1 + p_a = 2$. Here $h^0(\mathcal{O}_X(F)) = 0$ because F is a nonzero effective divisor. Let us prove that $h^1(\mathcal{O}_X(-F)) = 0$. From the exact sequence $0 \rightarrow \mathcal{O}_X(-F) \rightarrow \mathcal{O}_X \rightarrow \mathcal{O}_F \rightarrow 0$ of sheaves on X we obtain the exact sequence of cohomology groups

$$H^0(X, \mathcal{O}_X) \rightarrow H^0(X, \mathcal{O}_F) \rightarrow H^1(X, \mathcal{O}_X(-F)) \rightarrow H^1(X, \mathcal{O}_X).$$

Since F is reduced and connected, $H^0(X, \mathcal{O}_F)$ consists only of sections constant on F , and so the map from $H^0(X, \mathcal{O}_X)$ is surjective. On the other hand, $H^1(X, \mathcal{O}_X) = 0$ because X is a K3 surface. It follows that $H^1(X, \mathcal{O}_X(-F)) = 0$ as claimed, and therefore that $h^0(\mathcal{O}_X(-F)) = 2$.

The only maps whose fibers are elements of the linear system F are those associated to subseries of the complete linear system $|F|$. Since $\mathcal{O}_X(-F)$ has a 2-dimensional space of sections, the only nonconstant maps

of this kind are those associated to the complete linear system. This map is a fibration, for by hypothesis there is no curve contained in all divisors in the linear system $|F|$, so $F^2 = 0$ implies that no two fibers intersect. \square

Lemma 2.1.27 *For any 4-gon S we have $D_S^2 = 0$.*

Proof. Write $D_S = D_1 + D_2 + D_3 + D_4$, where the D_i are the geometric irreducible components of D_S . By Lemma 2.1.20 each D_i has self-intersection -2 . Also, $D_i \cdot D_{i+1} = 1$ and $D_i \cdot D_{i+2} = 0$, with indices read mod 4. The self-intersection of D_S is therefore $4 \cdot -2 + 4 \cdot 2 = 0$. \square

Lemma 2.1.28 *Let \mathcal{S} be an exhibit. Then there is an elliptic fibration of \bar{V} for which the lines in each 4-gon $S \in \mathcal{S}$ are the irreducible components of a fiber. Up to an automorphism of \mathbb{P}^1 this fibration is unique.*

Proof. By Proposition 2.1.2 the surface \bar{V} is a K3 surface. By Lemma 2.1.27 we have $D_S^2 = 0$ for any 4-gon $S \in \mathcal{S}$. By Lemma 2.1.25 the effective divisors D_S with $S \in \mathcal{S}$ are all contained in the same linear system. The lemma now follows immediately from Proposition 2.1.26. \square

Remark 2.1.29 Since the exhibits come in pairs, so do the elliptic fibrations mentioned in Lemma 2.1.28. By Remark 2.1.19 these pairs of fibrations are parametrized by the 15 pairs of elements in Ω .

It is known that generically the lines associated to the nodes and the tropes on the desingularized Kummer surface generate the full Néron-Severi group (see Remark 2.1.14). Together with Propositions 2.1.21 and 2.1.23, the following statement is slightly stronger.

Proposition 2.1.30 *If $\text{rk NS}(\bar{V}) = 17$, then the lines in Λ generate the full Néron-Severi group $\text{NS}(\bar{V})$.*

Proof. Let L denote the sublattice of $\text{NS}(\bar{V})$ generated by the elements of Λ . By Proposition 2.1.21, the lattice L has finite index in $\text{NS}(\bar{V})$. Suppose this index is not 1. Then from the equality $\text{disc } L = [\text{NS}(\bar{V}) : L]^2 \cdot \text{disc NS}(\bar{V})$, we find it is divisible by 2, and $\text{disc NS}(\bar{V})$ is a divisor of $64/2^2 = 16$.

Consider the transcendental lattice $T_{\bar{V}}$ of \bar{V} , which is the orthogonal complement of $\text{NS}(\bar{V})$ in $H^2(\bar{V}, \mathbb{Z})$. As the lattice $H^2(\bar{V}, \mathbb{Z})$ is unimodular, we have $|\text{disc } T_{\bar{V}}| = |\text{disc NS}(\bar{V})|$, so $\text{disc } T_{\bar{V}}$ is a divisor of 16 as well. However, since \bar{V} is isomorphic to the Kummer surface associated to the Jacobian J of the curve $y^2 = f(x)$ (see Remark 2.1.3), we find from [13], Prop. 4.3, that $T_{\bar{V}}$ is isomorphic to $T_J(2)$, the transcendental lattice of J , scaled by a factor of 2. Since $T_{\bar{V}}$ has rank $22 - 17 = 5$, its discriminant is divisible by $2^5 = 32$. From this contradiction we conclude that the index does equal 1. \square

2.2 Fields of definition

Recall that $T(F) = \{\xi \in A_F : \xi^2 = \delta\}$ for any field F for which δ is contained in A_F and that $l = k(\Omega)$ is the splitting field of f . Also recall that if $\omega \in F$ is a root of f , then φ_ω denotes the map $A_F \rightarrow F$ that sends $g(X)$ to $g(\omega)$. These maps induce the isomorphism $\varphi: A_l \rightarrow \bigoplus_{\omega \in \Omega} l$ given by $X \mapsto (\varphi_\omega(X))_\omega = (\omega)_\omega$.

Lemma 2.2.1 *For any $\xi \in T(\bar{k})$ and $\omega, \psi \in \Omega$ we have $\varphi_\psi(P_{\xi, \omega}) = 0$ if and only if $\psi = \omega$.*

Proof. This follows from the definition of $P_{\xi, \omega}$ and the fact that $\xi \in \bar{A}$ is a unit. \square

For any object Y to which we can apply every Galois automorphism in $G(\bar{k}/k)$ we will say that Y is defined over the field extension $k' \subset \bar{k}$ of k if for all $\sigma \in G(\bar{k}/k')$ we have $^\sigma Y = Y$. The smallest field over which Y is defined will be called the field of definition of Y and denoted by $k(Y)$. Note that every element of $\tilde{T}(k')$ is defined over k' , even though it may be represented by an element in $T(k')$ that is only defined over a quadratic extension of k' . Note that if $Y = (y_1, \dots, y_n)$ is a sequence, then $k(Y)$ is the composition of all the $k(y_i)$. If $Z = \{z_1, \dots, z_n\}$ is a set, then $k(Z)$ may be strictly smaller than the field of definition of the sequence (z_1, \dots, z_n) , a field that we will denote by $k([Z])$.

Lemma 2.2.2 *Inside \bar{k} we have $l \cdot k(L) = k([\Lambda])$ for all $L \in \Lambda$.*

Proof. Suppose $\sigma \in G(\bar{k}/k)$ acts trivially on Λ . Then for all $\omega \in \Omega$ and $\xi \in T(\bar{k})$ the automorphism σ fixes the intersection point $P_{\xi, \omega}$ of L_ξ and $\zeta_\omega L_\xi$. The point $P_{\xi, \omega}$ determines ω uniquely by Lemma 2.2.1. We conclude that σ fixes all $\omega \in \Omega$, so σ fixes l and l is contained in $k([\Lambda])$. Clearly we also have $k(L) \subset k([\Lambda])$, so we find $l \cdot k(L) \subset k([\Lambda])$. For every other $L' \in \Lambda$ there is a $\zeta \in \mu(A_l)$ such that $\zeta L = L'$. As the automorphism $[\zeta]$ is defined over l , we find that L' is defined over $l \cdot k(L)$, so $k(L') \subset l \cdot k(L)$. This holds for all $L' \in \Lambda$ so we find $k([\Lambda]) \subset l \cdot k(L)$ and thus $k([\Lambda]) = l \cdot k(L)$. \square

For every ω we fix a square root $\sqrt{\delta_\omega}$ of $\delta_\omega = \varphi_\omega(\delta)$ in \bar{k} , yielding also a fixed square root $\xi_0 = \varphi^{-1}((\sqrt{\delta_\omega})_{\omega \in \Omega})$ of δ . Note that with the Legendre polynomials P_ω of Remark 2.1.1 we can write $\xi_0 = \sum_\omega \sqrt{\delta_\omega} P_\omega$. We define the fields

$$m' = l(\{\sqrt{\delta_\omega} : \omega \in \Omega\}), \quad \text{and} \quad m = l(\{\sqrt{\delta_\omega} \sqrt{\delta_\psi} : \omega, \psi \in \Omega\}).$$

The square root ξ_0 of δ trivializes the torsors T and \tilde{T} under μ_A and $\tilde{\mu}$ respectively, identifying $\zeta \in \mu_A(\bar{k}) = \mu(\bar{A})$ with $\zeta \xi_0 \in T(\bar{k})$. By Remark 2.1.9 the k -torsors $\tilde{T}(\bar{k})$ and $\Lambda(\bar{k})$ under $\tilde{\mu}(\bar{k})$ are isomorphic over k as well, identifying the class of ξ in $\tilde{T}(\bar{k})$ with the line L_ξ . Just after Lemma 2.1.10 we identified the subset $I \subset \Omega$ with the element $\zeta_I \in \mu_A(\bar{k})$. Similarly, we write $\xi_I = \zeta_I \xi_0$. We also set $L_0 = L_{\xi_0}$ and write $L_I = \zeta_I L_0 = L_{\xi_I}$. Note that $L_I = L_{\Omega-I}$.

Lemma 2.2.3 *Fix $\sigma \in G(\bar{k}/k)$. Then ${}^\sigma L_0 = L_I$ if and only if I or $\Omega - I$ equals*

$$\{\sigma_\omega : \omega \in \Omega, \sigma \sqrt{\delta_\omega} = \sqrt{\delta_{\sigma\omega}}\}.$$

Proof. This follows immediately from Lemma 2.1.7 and the equation

$${}^\sigma \xi_0 = \varphi^{-1} \left(\left(\sigma \sqrt{\delta_{\sigma^{-1}\omega}} \right)_{\omega \in \Omega} \right) = \zeta_J \xi_0,$$

where J is the set given in the lemma. \square

Lemma 2.2.4 *We have $k([\Lambda]) = m$.*

Proof. For every $\psi \in \Omega$ the element $\sqrt{\delta_\psi} \xi_0 = \sum_\omega \sqrt{\delta_\psi} \sqrt{\delta_\omega} P_\omega$ is defined over m , where P_ω is the Legendre polynomial introduced in Remark 2.1.1. The line L_0 corresponds to the subspace $\{(\sqrt{\delta_\psi} \xi_0)^{-1}(sX + t) : s, t \in m\}$ of A_m , so L_0 is defined over m as well and we have $k(L_0) \subset m$. From Lemma 2.2.2 we deduce $k([\Lambda]) \subset m$. For the converse, consider $\sigma \in G(\bar{k}/k([\Lambda]))$. From Lemma 2.2.3 and the equation $L_0 = {}^\sigma L_0$ we find that either we have $\sigma \sqrt{\delta_\omega} = \sqrt{\delta_\omega}$ for all ω , or we have $\sigma \sqrt{\delta_\omega} = -\sqrt{\delta_\omega}$ for all ω . In both cases we find that σ acts trivially on m , so we also have $m \subset k([\Lambda])$. \square

Lemma 2.2.5 *Let $\mathcal{S} = \{S_1, S_2\}$ be a gallery. Then there are $\omega, \psi \in \Omega$ such that we have*

$$k(\mathcal{S}) = k(\omega + \psi, \omega\psi) \quad \text{and} \quad k(S_1) = k(S_2) = k\left(\omega + \psi, \omega\psi, \prod_{\theta \in \Omega \setminus \{\omega, \psi\}} \sqrt{\delta_\theta}\right).$$

Proof. Let ω, ψ be such that the 4-gons in the S_i are orbits under $\Phi_{\omega\psi}$. Write $k' = k(\omega + \psi, \omega\psi)$ and suppose we have $\sigma \in G(\bar{k}/k')$. Then σ fixes the polynomial $(x - \omega)(x - \psi)$, so it permutes ω and ψ . Therefore, σ permutes the orbits under $\Phi_{\omega\psi}$, which are the 4-gons in $S_1 \cup S_2$ (compare Lemma 2.1.17). Since every 4-gon is contained in a unique gallery, this implies that σ fixes \mathcal{S} , so we have $k(\mathcal{S}) \subset k'$. For the converse, suppose we have $\sigma \in G(\bar{k}/k(\mathcal{S}))$. Then σ permutes the intersection points among any two lines in the same 4-gon in $S_1 \cup S_2$. These intersection points are all of the form $P_{\xi, \omega}$ or $P_{\xi, \psi}$ for some $\xi \in T(\bar{k})$. By Lemma 2.2.1 this implies that σ permutes ω and ψ , so it acts trivially on k' and we find $k' \subset k(\mathcal{S})$, so $k' = k(\mathcal{S})$. For the

second equality, set $N = \prod_{\theta \in \Omega \setminus \{\omega, \psi\}} \sqrt{\delta_\theta}$ and consider $\sigma \in G(\bar{k}/k')$. Then σ fixes \mathcal{S} , so it permutes \mathcal{S}_1 and \mathcal{S}_2 , and σ sends N to $\pm N$. Let n denote the number of $\theta \in \Omega \setminus \{\omega, \psi\}$ for which we have $\sigma\sqrt{\delta_\theta} = -\sqrt{\delta_\theta}$. Then σ fixes N if and only if n is even. Let $I \subset \Omega$ be such that ${}^\sigma\xi_0 = \xi_I\xi_0$. Then we have $n = \#I \cap \Omega \setminus \{\omega, \psi\}$ and ${}^\sigma L_0 = L_I$. Suppose that $n = 0$ or $n = 4$. Then L_0 and ${}^\sigma L_0 = L_I$ are in the same orbit under $\Phi_{\omega\psi}$, so in the same 4-gon in $\mathcal{S}_1 \cup \mathcal{S}_2$. By Lemma 2.1.17 each 4-gon is contained in a unique exhibit, so σ fixes \mathcal{S}_1 or \mathcal{S}_2 , and thus both. Now suppose $n \in \{1, 2, 3\}$. Then ${}^\sigma L_0$ is in a different orbit under $\Phi_{\omega\psi}$ than L_0 . By Lemma 2.1.16 the number n is odd if and only if the line L_0 intersects some line in the orbit of ${}^\sigma L_0$, which, by Lemma 2.1.17, happens if and only if L_0 and ${}^\sigma L_0$ are in opposite exhibits. We conclude that for all n the automorphism σ fixes \mathcal{S}_1 and \mathcal{S}_2 if and only if n is even, so if and only if σ fixes N . This implies that $k(\mathcal{S}_1) = k(\mathcal{S}_2) = k'(N)$. \square

Remark 2.2.6 The first equality of Lemma 2.2.5 is not surprising as we already saw in Remark 2.1.19 that galleries are parametrized by pairs of elements in Ω . Note that $k' = k(\mathcal{S}) = k(\omega + \psi, \omega\psi)$ is the smallest field over which f factors as $f = f_2 f_4$, where f_2 has degree 2 and roots ω and ψ . It is the field of definition of the 2-torsion point $(\omega, 0) + (\psi, 0) - 2 \cdot \infty$ on the Jacobian of the curve $y^2 = f(x)$. If we set $A_4 = k'[X]/f_4$ and we let δ' denote the image of δ under the natural map $A_{k'} \rightarrow A_4$ then the element $\prod_{\theta} \sqrt{\delta_\theta}$ in Lemma 2.2.5 is a square root of the norm $N_{A_4/k'} \delta'$ of δ' from A_4 to k' . The two elliptic fibrations associated to \mathcal{S}_1 and \mathcal{S}_2 in Lemma 2.1.28 are also defined over the field $k(\mathcal{S}_1) = k(\mathcal{S}_2) = k'(\sqrt{N_{A_4/k'} \delta'})$. We will say that these are the elliptic fibrations associated to the pair (ω, ψ) , or to the factorization $f = f_2 f_4$. The 4-gons in \mathcal{S}_1 and \mathcal{S}_2 that make up the fibers of these fibrations are orbits of Λ under the group $\Phi_{\omega\psi}$. In section 2.3 we will find explicit equations for these fibrations.

Let Λ_1 and Λ_2 be the two maximal subsets S of Λ for which all lines in S have the same parity.

Lemma 2.2.7 *We have $k(\Lambda_1) = k(\Lambda_2) = k(\sqrt{N(\delta)})$, where $N = N_{A/k}$ is the norm from A to k .*

Proof. Take $\sigma \in G(\bar{k}/k)$. Let $I \subset \Omega$ be such that ${}^\sigma\xi_0 = \xi_I$, and set $n = \#I$. The automorphism σ permutes Λ_1 and Λ_2 , so it fixes both if and only if L_0 and ${}^\sigma L_0 = L_I$ have the same parity, i.e., if and only if n is even. Note that n also equals the number of $\omega \in \Omega$ with $\sigma\sqrt{\delta_\omega} = -\sqrt{\delta_\omega}$, so n is even if and only if σ fixes the element $\prod_{\omega} \sqrt{\delta_\omega} = \sqrt{N(\delta)}$. We conclude that σ fixes Λ_1 and Λ_2 if and only if σ fixes $\sqrt{N(\delta)}$, which shows that $k(\Lambda_1) = k(\Lambda_2) = k(\sqrt{N(\delta)})$. \square

Let $\text{Aut } \Lambda$ denote the group of permutations of Λ that respect the intersection pairing. Let $\rho: G(\bar{k}/k) \rightarrow \text{Aut } \Lambda$ be the corresponding Galois representation.

Lemma 2.2.8 *The kernel of the representation $\rho: G(\bar{k}/k) \rightarrow \text{Aut } \Lambda$ is $G(\bar{k}/m)$.*

Proof. This follows from Lemma 2.2.4. \square

Proposition 2.2.9 *All extensions among the fields $k \subset l \subset m \subset m'$ are Galois and we have exact sequences*

$$\begin{aligned} 1 &\rightarrow \text{Gal}(m'/m) \rightarrow \text{Gal}(m'/l) \rightarrow \text{Gal}(m/l) \rightarrow 1 \\ 1 &\rightarrow \text{Gal}(m/l) \rightarrow \text{Gal}(m/k) \rightarrow \text{Gal}(l/k) \rightarrow 1 \\ 1 &\rightarrow \text{Gal}(m'/m) \rightarrow \text{Gal}(m'/l) \rightarrow \text{Gal}(m/k) \rightarrow \text{Gal}(l/k) \rightarrow 1. \end{aligned}$$

Proof. The extension l/k is normal because l is the splitting field of f over k , and separable because f is. Since $[m' : l] = 64 = 2^6$, and we have assumed that $\text{char } k \neq 2$, the extension m'/k and all subextensions are separable. The group $\text{Gal}(\bar{k}/m)$ is normal in $\text{Gal}(\bar{k}/k)$ because it is the kernel of ρ by Lemma 2.2.8. This means that m/k is Galois, and therefore so is m/l . Similarly, the group $\text{Gal}(\bar{k}/m')$ is normal in $\text{Gal}(\bar{k}/k)$ because it is the kernel of the representation $\text{Gal}(\bar{k}/k) \rightarrow \text{Aut } T(\bar{k})$. This implies that m'/k is Galois, which also follows from the fact that m' is obtained from l by adjoining a square root of an element in l as well as the square roots of all conjugates of that element under $\text{Gal}(l/k)$. Therefore, the extensions m'/m and

m'/l are Galois, too. The first two exact sequences are the standard short exact sequences of Galois groups associated to the double extensions $k \subset l \subset m$ and $l \subset m \subset m'$. They can be combined to give the last sequence. \square

Example 2.2.10 Let F be any field and define the generic fields

$$\begin{aligned} m'_g &= F(\omega_1, \dots, \omega_6, d_0, \dots, d_5)[T_1, \dots, T_6] / \left(T_j^2 - \sum_{i=0}^5 d_i \omega_j^i : 1 \leq j \leq 6 \right), \\ m_g &= F(\omega_1, \dots, \omega_6, d_0, \dots, d_5, \{\epsilon_i \epsilon_j : 1 \leq i, j \leq 6\}), \\ l_g &= F(\omega_1, \dots, \omega_6, d_0, \dots, d_5), \\ k_g &= F(s_1, \dots, s_6, d_0, \dots, d_5), \end{aligned}$$

where $\omega_1, \dots, \omega_6, d_1, \dots, d_6$ are independent transcendentals, s_j denotes the elementary symmetric polynomial of degree j in the variables $\omega_1, \dots, \omega_6$, and ϵ_j is the image of T_j in m'_g . We have $k_g \subset l_g \subset m_g \subset m'_g$. Set

$$f = \prod_{j=1}^6 (X - \omega_j) = X^6 - s_1 X^5 + s_2 X^4 - s_3 X^3 + s_2 X^4 - s_5 X^5 + s_6 \in k_g[X],$$

and define $A = k_g[X]/f$. By abuse of notation we will also write X for the image of X in A . Set $\delta = \sum_{i=0}^5 d_i X^i \in A$. The evaluation maps $\varphi_j: A \rightarrow l_g$ sending X to ω_j induce an isomorphism $\varphi: A_{l_g} \rightarrow \bigoplus_{j=1}^6 l_g$. We have $\epsilon_j^2 = \delta_j$ with $\delta_j = \varphi_j(\delta)$, so the fields l_g , m_g , and m'_g depend on k_g , f and δ exactly as the corresponding fields without the subscript g for “generic” did before, abbreviating ω_j to j in any index. We will give explicit equations for the intersection points of the lines in Λ_g in this generic situation. As in Remark 2.1.1, let P_j denote the Legendre polynomial $P_j = \prod_{i \neq j} (X - \omega_i) / (\omega_j - \omega_i) \in A_{l_g}$ for $1 \leq j \leq 6$. Then φ^{-1} sends $(c_j)_{j=1}^6$ to $\sum_{j=1}^6 c_j P_j$. Set $\xi_0 = \varphi^{-1}((\epsilon_j)_j) = \sum_{j=1}^6 \epsilon_j P_j$. Then we have $\xi_0^2 = \delta$. Let $b_{ji} \in F(\omega_1, \dots, \omega_6)$ be such that $P_j = \sum_{i=0}^5 a_{ji} X^i$. In A_{l_g} we have $XP_j = \omega_j P_j$, so we find that the coordinates of the point P_{ϵ_0, ω_r} in terms of the a_i are given by the coefficients of

$$\xi_0^{-1}(X - \omega_r) = \sum_{j=1}^6 \epsilon_j^{-1}(X - \omega_r) P_j = \sum_{j=1}^6 \epsilon_j^{-1}(\omega_j - \omega_r) P_j = \sum_{i=0}^5 \left(\sum_{j=1}^6 \epsilon_j^{-1}(\omega_j - \omega_r) b_{ji} \right) X^i.$$

Multiplying all the coefficients by one of the ϵ_j^{-1} shows that the point P_{ξ_0, ω_r} is indeed defined over m_g . All other intersection points are obtained by replacing some of the ϵ_j by their negatives and r by some $r' \in \{1, \dots, 6\}$. By specialization, these formulas give explicit equations for the intersection points of the lines in Λ over any field. This also gives all the lines. Note that the group $\text{Gal}(m'_g/l_g)$ is isomorphic to $\bigoplus_{j=1}^6 \mathbb{Z}/2\mathbb{Z}$, where the generator of the j -th component sends ϵ_j to $-\epsilon_j$. The group $\text{Gal}(m'_g/m_g) \cong \mathbb{Z}/2\mathbb{Z}$ embeds diagonally into $\text{Gal}(m'_g/l_g)$, sending every ϵ_j to $-\epsilon_j$. Hence, the group $\Gamma = \text{Gal}(m_g/l_g)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^6 / (\mathbb{Z}/2\mathbb{Z})$. The group $\text{Gal}(l_g/k_g)$ is isomorphic to S_6 . There is a section ι' of the homomorphism $\text{Gal}(m'_g/k_g) \rightarrow \text{Gal}(l_g/k_g)$ that sends an element $\sigma \in \text{Gal}(l_g/k_g)$ to the unique lift that sends the set $\{\epsilon_1, \dots, \epsilon_6\}$ to itself. The composition ι of ι' and the restriction map $\text{Gal}(m'_g/k_g) \rightarrow \text{Gal}(m_g/k_g)$ is a section of the homomorphism $\text{Gal}(m_g/k_g) \rightarrow \text{Gal}(l_g/k_g)$. Through ι the group $\text{Gal}(l_g/k_g) \cong S_6$ acts on Γ by conjugation. This action is induced by permutation of the components of $\bigoplus_{j=1}^6 \mathbb{Z}/2\mathbb{Z} = \text{Gal}(m'_g/l_g)$ in the obvious way. Since the middle sequence of Proposition 2.2.9 splits in this generic case, we find that $\text{Gal}(m_g/k_g)$ is isomorphic to the semidirect product $\Gamma \rtimes S_6$, which has $32 \cdot 6! = 23040$ elements.

Proposition 2.2.11 *Generically, the representation $\rho: \text{Gal}(\bar{k}/k) \rightarrow \text{Aut } \Lambda$ is surjective.*

Proof. It suffices to show that ρ is surjective in the case of the generic situation of Example 2.2.10, so suppose we are in that case. We will use the same notation as in Example 2.2.10, including abbreviating ω_j to j in

indices of lines and points. Take any $\tau \in \text{Aut } \Lambda_g$ and consider the line $L_0 = L_{\xi_0}$. Since $\Gamma = \text{Gal}(m_g/l_g)$ acts transitively on Λ_g , there is a $\sigma_1 \in \Gamma$ with $\rho(\sigma_1)(L_0) = \tau(L_0)$. Then $\tau' = \rho(\sigma_1)^{-1}\tau$ fixes L_0 , so it permutes the six lines L_j that intersect L_0 . The corresponding six intersection points are P_{ξ_0, ω_j} for $1 \leq j \leq 6$, so τ' induces a unique permutation of the ω_j by Lemma 2.2.1, which corresponds to an element $\psi \in \text{Gal}(l_g/k_g)$. Set $\sigma_2 = \iota'(\psi)$. Then σ_2 sends the set $\{\epsilon_1, \dots, \epsilon_6\}$ to itself, so it fixes $\xi_0 = \sum_{j=1}^6 \epsilon_j P_j$ as both the ϵ_j and the P_j are acted on according to their indices. This implies that $\rho(\sigma_2)$ fixes L_0 , while it permutes the intersection points P_{ξ_0, ω_j} in the same way τ' does. Therefore $\tau'' = \rho(\sigma_2)^{-1}\tau'$ fixes L_0 and the six lines L_j . For $i \neq j$ the line L_{ij} is the unique line that intersects L_i and L_j that is not equal to L_0 . This implies that τ'' also fixes L_{ij} . Similarly, the line L_{ijr} is the unique line that intersects both L_{ij} and L_{ir} that is not equal to L_i . This implies that τ'' also fixes L_{ijr} . We conclude that τ'' is the identity, so $\tau = \rho(\sigma_1\sigma_2)$ and ρ is surjective. \square

By Lemma 2.2.8 and Proposition 2.2.11 the generic representation $\rho_g: \Gamma \rtimes S_6 \cong \text{Gal}(m_g/k_g) \rightarrow \text{Aut } \Lambda_g \cong \text{Aut } \Lambda$ is an isomorphism. We will denote the composition $\rho_g \circ \iota: S_6 \rightarrow \text{Aut } \Lambda$ by ι as well.

It will be useful to have names for the elements of $\text{Aut } \Lambda$. For every set $I \subset \Omega$, let $s_I \in \text{Aut } \Lambda$ denote the permutation induced by $[\zeta_I]$. Note we have $s_I = s_{\Omega \setminus I}$ and s_I and s_J commute for every $I, J \subset \Omega$. For any permutation $\sigma \in S_6 = \text{Sym}(\Omega)$, let t_σ denote the permutation that sends L_I to $L_{\sigma I}$. For $\sigma, \tau \in S_6$ we have $t_\sigma \circ t_\tau = t_{\sigma\tau}$, and

$$t_\sigma \circ s_I = s_{\sigma I} \circ t_\sigma. \quad (1)$$

Note that the action of S_6 on Λ that we have defined depends on the choice of L_0 , or the $\sqrt{\delta_\omega}$, just as the section ι in Example 2.2.10 depends on the choice of the square roots ϵ_j of the δ_j . We will state some of the following lemmas under an extra condition on L_0 , knowing that the general case may always be obtained by changing some of the $\sqrt{\delta_\omega}$ to their negatives and changing the L_I and t_σ accordingly. By specialization of the generic $\omega_j \in m'_g$ of Example 2.2.10 to the $\omega \in \Omega$, and the ϵ_j to the corresponding $\sqrt{\delta_\omega}$, we specialize k_g, l_g, m_g, Λ_g , and the corresponding generic representation ρ_g to k, l, m, Λ , and ρ respectively. Let r denote the associated injective map from $\text{Gal}(m/k)$ to $\text{Gal}(m_g/k_g)$. Then we have the following commutative diagram.

$$\begin{array}{ccc} \text{Gal}(m_g/k_g) & \xrightarrow[\cong]{\rho_g} & \text{Aut } \Lambda_g \\ \uparrow r & & \uparrow \cong \\ \text{Gal}(m/k) & \xrightarrow{\rho} & \text{Aut } \Lambda \end{array}$$

Lemma 2.2.12 *Let H be a subgroup of $\text{Aut } \Lambda$ and let H_g be the corresponding subgroup of $\text{Aut } \Lambda_g$. Then the fixed field of $\rho^{-1}H$ is exactly the specialization of the fixed field of $\rho_g^{-1}H_g$.*

Proof. Set $H' = \rho^{-1}H$ and $H'_g = \rho_g^{-1}H_g$. By the commutative diagram above we have $r^{-1}(H'_g) = H'$. For every specialization k' of a subextension k'_g of m_g over k_g , we have $\text{Gal}(m/k') = r^{-1}(\text{Gal}(m_g/k'_g))$. In other words, the fixed field of $H' = r^{-1}(H'_g)$ is exactly the specialization of the fixed field of H'_g . \square

For any $\omega, \psi \in \Omega$, let $\Psi_{\omega\psi}$ denote the group generated by s_ω and s_ψ . Then $\Phi_{\omega\psi}$ acts on Λ through $\Psi_{\omega\psi}$. For any exhibit \mathcal{S} , let $G_{\mathcal{S}}$ denote the maximal subgroup of $\text{Aut } \Lambda$ that fixes \mathcal{S} and let $G_{[\mathcal{S}]}$ denote the maximal subgroup that fixes all 4-gons in \mathcal{S} . We will use Lemma 2.2.12 to find generators of $k([\mathcal{S}])$, the compositum of the fields $k(S)$ for all S in some exhibit \mathcal{S} . This field will be used in Section 2.3 to find explicit equations for the elliptic fibration associated to \mathcal{S} in Lemma 2.1.28.

Lemma 2.2.13 *For any exhibit \mathcal{S} the group $G_{\mathcal{S}}$ has order 768 and the natural homomorphism from $G_{\mathcal{S}}$ to the group $\text{Sym}(\mathcal{S})$ of permutations of the 4-gons in \mathcal{S} is surjective. Its kernel is $G_{[\mathcal{S}]}$.*

Proof. In the generic case of Example 2.2.10, the field $k_g(\mathcal{S})$ has degree 30 by Lemma 2.2.5. Therefore the group $\text{Gal}(m_g/k_g(\mathcal{S}))$ has order $23040/30 = 768$. By Lemma 2.2.8 and Proposition 2.2.11, the representation

$\rho_g: \text{Gal}(m_g/k_g) \rightarrow \text{Aut } \Lambda_g$ is an isomorphism, so we find that G_S has order 768 as well. Clearly the kernel of the homomorphism $\chi: G_S \rightarrow \text{Sym}(\mathcal{S})$ equals $G_{[\mathcal{S}]}$. Let ω and ψ be such that the 4-gons in \mathcal{S} are orbits under $\Phi_{\omega\psi}$, and set $H = \{t_\sigma : \sigma \in \text{Sym}(\Omega \setminus \{\omega, \psi\})\} \subset \text{Aut } \Lambda$. Each $h \in H$ sends orbits under the group $\Phi_{\omega\psi}$ to orbits under the same group, and as we have $h(L_0) = L_0$, the permutation h fixes at least one of these orbits, so it fixes the two complementary exhibits associated to the pair (ω, ψ) . We deduce $H \subset G_S$. Without loss of generality we will assume that L_0 is not contained in any of the 4-gons of \mathcal{S} . Then by Lemma 2.1.17, for each 4-gon S in \mathcal{S} there is a $\theta \in \Omega \setminus \{\omega, \psi\}$ such that S is the orbit of L_θ . It follows that each permutation of \mathcal{S} is induced by a permutation of $\Omega \setminus \{\omega, \psi\}$, so the restriction of χ to H is surjective, which implies that χ is surjective. \square

Lemma 2.2.14 *Let \mathcal{S} be an exhibit, let $\omega, \psi \in \Omega$ be such that the 4-gons of \mathcal{S} are orbits under $\Phi_{\omega\psi}$, and assume that L_0 is contained in one of the 4-gons of \mathcal{S} . Let $\theta_1, \theta_2, \theta_3, \theta_4$ be the elements of $\Omega \setminus \{\omega, \psi\}$. Then $G_{[\mathcal{S}]}$ is generated by s_ω, s_ψ , and t_σ for $\sigma \in \langle (\omega \psi), (\theta_1 \theta_2)(\theta_3 \theta_4), (\theta_1 \theta_3)(\theta_2 \theta_4) \rangle$.*

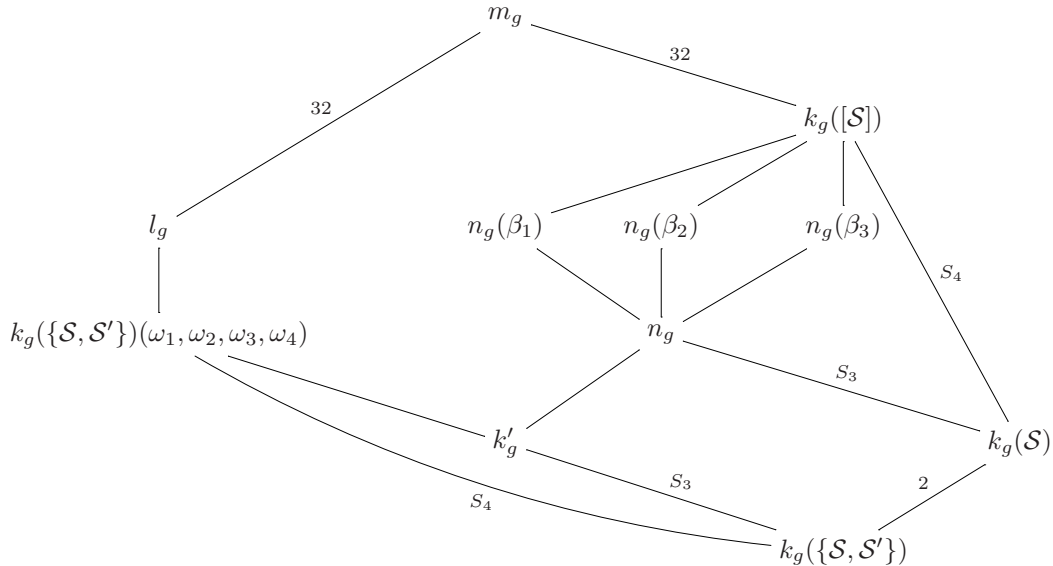
Proof. Set $B = \langle (\theta_1 \theta_2)(\theta_3 \theta_4), (\theta_1 \theta_3)(\theta_2 \theta_4) \rangle$ and let H denote the subgroup of $\text{Aut } \Lambda$ generated by $s_\omega, s_\psi, t_{(\omega \psi)}$, and t_σ for $\sigma \in B$. Note that every $\sigma \in B$ fixes ω and ψ . By (1) this implies that for every $h \in H$ we have $h\Psi_{\omega\psi}h^{-1} = \Psi_{\omega\psi}$, so h sends orbits under $\Psi_{\omega\psi}$ to orbits under $\Psi_{\omega\psi}$, i.e., h permutes the 4-gons in \mathcal{S} and its complementary exhibit. The elements s_ω, s_ψ , and $t_{(\omega \psi)}$ fix each of these 4-gons. Let $S \in \mathcal{S}$ be the 4-gon containing L_0 . We have $t_\sigma(L_0) = L_0$ for all $\sigma \in B$, so h sends S to S for all $h \in H$. Let $S' \in \mathcal{S}$ be a different 4-gon. Then by Lemma 2.1.17 there are $\theta, \theta' \in \Omega \setminus \{\omega, \psi\}$ such that $s_{\theta\theta'}(S) = S'$. For each $\sigma \in B$ we have

$$t_\sigma(s_{\theta\theta'}(L_0)) = s_{\sigma(\theta\theta')}(t_\sigma(L_0)) = s_{\sigma(\theta\theta')}(L_0).$$

For all $\sigma \in B$ we have $s_{\theta\theta'}S = s_{\sigma(\theta\theta')}S$, so t_σ also fixes S' . We conclude $H \subset G_{[\mathcal{S}]}$. By Lemma 2.2.13 the order of $G_{[\mathcal{S}]}$ equals $768/4! = 32 = \#H$, so we have $H = G_{[\mathcal{S}]}$. \square

We can now find explicit generators of the field $k([\mathcal{S}])$ in the generic case.

Lemma 2.2.15 *Consider the generic case of Example 2.2.10. Let $\{\mathcal{S}, \mathcal{S}'\}$ be a gallery, such that the 4-gons of \mathcal{S} are orbits under $\Phi_{\omega_5\omega_6}$, and assume that L_0 is contained in one of the 4-gons of \mathcal{S} . Set $N = \epsilon_1\epsilon_2\epsilon_3\epsilon_4$, $\alpha_1 = \omega_1\omega_4 + \omega_2\omega_3$, $\alpha_2 = \omega_1\omega_3 + \omega_2\omega_4$, $\alpha_3 = \omega_1\omega_2 + \omega_3\omega_4$, $\beta_1 = \epsilon_1\epsilon_4 + \epsilon_2\epsilon_3$, $\beta_2 = \epsilon_1\epsilon_3 + \epsilon_2\epsilon_4$, and $\beta_3 = \epsilon_1\epsilon_2 + \epsilon_3\epsilon_4$. Then $k'_g = k_g(\omega_5 + \omega_6, \omega_5\omega_6, \alpha_1, \alpha_2, \alpha_3)$ is the unique S_3 -extension of $k_g(\{\mathcal{S}, \mathcal{S}'\}) = k_g(\omega_5 + \omega_6, \omega_5\omega_6)$ contained in the S_4 -extension $k_g(\{\mathcal{S}, \mathcal{S}'\})(\omega_1, \omega_2, \omega_3, \omega_4)$. Set $n_g = k'_g(N)$. Then the field $k_g([\mathcal{S}])$ equals $n_g(\beta_1, \beta_2, \beta_3)$ and is an S_4 -extension of $k_g(\mathcal{S}) = k_g(\{\mathcal{S}, \mathcal{S}'\})(N)$. Its unique S_3 -subextension is n_g , and its unique quadratic subextensions of n_g are generated by the β_i .*



Proof. The first statement is elementary Galois theory. The field $k_g([S])$ is the fixed field of the group $\rho_g^{-1}(G_{[S]})$. By Lemma 2.2.13 this field is an S_4 -extension of the fixed field $k_g(\mathcal{S})$ of $G_{\mathcal{S}}$, which equals $k_g(\omega_5 + \omega_6, \omega_5\omega_6, N) = k_g(\{\mathcal{S}, \mathcal{S}'\})(N)$ by Lemma 2.2.5. Using Lemma 2.2.14 one checks that the group $\rho_g^{-1}(G_{[S]})$ acts trivially on $n_g(\beta_1, \beta_2, \beta_3)$, so we conclude $n_g(\beta_1, \beta_2, \beta_3) \subset k_g([S])$. Since k'_g and $k_g(\mathcal{S})$ intersect in $k_g(\{\mathcal{S}, \mathcal{S}'\})$, we find that the compositum n_g is an S_3 -extension of $k_g(\mathcal{S})$, and therefore the unique S_3 -extension contained in $k_g([S])$. By elementary Galois theory and group theory this implies that there are three quadratic extensions of n_g contained in $k_g([S])$. Note that $\rho_g^{-1}(s_{\omega_1\omega_4})$ and $\rho_g^{-1}(s_{\omega_1\omega_3})$ act trivially on $n_g(\beta_1)$ and $n_g(\beta_2)$ respectively, but nontrivially on β_2 and β_1 respectively. We conclude that β_1 and β_2 generate two different quadratic extensions of n_g . By symmetry, β_3 generates a third. This implies $[n_g(\beta_1, \beta_2, \beta_3) : n_g] \geq 4 = [k_g([S]) : n_g]$, so we deduce that $k_g([S]) = n_g(\beta_1, \beta_2, \beta_3)$. \square

The generators of the field $k([S])$ in any other special case follow immediately.

Corollary 2.2.16 *Let the notation be as in Lemma 2.2.14. Set $N = \sqrt{\delta_1\delta_2\delta_3\delta_4}$, $\alpha_1 = \theta_1\theta_4 + \theta_2\theta_3$, $\alpha_2 = \theta_1\theta_3 + \theta_2\theta_4$, $\alpha_3 = \theta_1\theta_2 + \theta_3\theta_4$, $\beta_1 = \sqrt{\delta_1\delta_4} + \sqrt{\delta_2\delta_3}$, $\beta_2 = \sqrt{\delta_1\delta_3} + \sqrt{\delta_2\delta_4}$, and $\beta_3 = \sqrt{\delta_1\delta_2} + \sqrt{\delta_3\delta_4}$. Then $k_g([S])$ equals*

$$k(\omega + \psi, \omega\psi, N, \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3).$$

Proof. Since $k_g([S])$ is the fixed field of the group $\rho^{-1}(G_{[S]})$, it follows from Lemma 2.2.12 that it suffices to do this in the generic case. This is dealt with in Lemma 2.2.15. \square

2.3 The elliptic fibrations

Let $\mathcal{S} = \{S_1, S_2, S_3, S_4\}$ and $\mathcal{S}' = \{S_5, S_6, S_7, S_8\}$ be complementary exhibits. By Lemma 2.1.28 there is an elliptic fibration $\bar{V} \rightarrow \mathbb{P}^1$ such that the 4-gons in \mathcal{S} are some of the fibers. For any $S \in \mathcal{S}$ this fibration can be defined over the field $k(S)$. It is possible, however, that none of the fibers is defined over the field $k(\mathcal{S})$. This implies that the base of the family of fibers is not isomorphic to \mathbb{P}^1 over $k(\mathcal{S})$. As the base curve does become isomorphic to \mathbb{P}^1 over some extension field, it is isomorphic to a conic. In this section we will give explicit equations, both for such a conic and for the fibration map in the generic case of Example 2.2.10. We will use the notation introduced in that example. The equations for any special case follow by specialization. Although the expressions involved become quite large, all computations in this section can still be checked by hand. We recommend, however, to check them with the MAGMA script provided [21]. We will first give the elliptic fibration over the field $k_g([S])$, over which the base curve can be taken to be the projective line.

2.3.1 A fibration over the projective line

After renumbering the elements of Ω , we may assume that the 4-gons of \mathcal{S} are orbits under $\Phi_{\omega_5\omega_6}$. After applying an automorphism that sends some of the ϵ_i to $-\epsilon_i$ (for notation, see Example 2.2.10), we may also assume that L_0 is contained in one of the 4-gons of \mathcal{S} . We renumber S_1, \dots, S_4 and S_5, \dots, S_8 , so that S_1, \dots, S_8 contain the lines $L_{14}, L_{24}, L_{34}, L_0, L_1, L_2, L_3$, and L_4 respectively. In particular this means

$$\begin{aligned} S_1 &= \{L_{14}, L_{23}, L_{145}, L_{235}\}, & S_5 &= \{L_1, L_{15}, L_{16}, L_{156}\}, \\ S_2 &= \{L_{13}, L_{24}, L_{135}, L_{245}\}, & S_6 &= \{L_2, L_{25}, L_{26}, L_{256}\}. \end{aligned}$$

For notational convenience, we let N , α_i and β_i be as in Lemma 2.2.15. We also set

$$\begin{aligned} \gamma_1 &= \alpha_3 - \alpha_2, & \Delta_4 &= \prod_{1 \leq i < j \leq 4} (\omega_i - \omega_j), \\ \gamma_2 &= \alpha_1 - \alpha_3, & \kappa_j &= \prod_{1 \leq i \leq 4, i \neq j} (\omega_j - \omega_i), & 1 \leq j \leq 4, \\ \gamma_3 &= \alpha_2 - \alpha_1, & \eta &= \sum_{i=1}^4 \epsilon_i, \\ c_r &= \text{elementary symmetric polynomial in the } \omega_j \text{ (} 1 \leq j \leq 4 \text{) of degree } r. \end{aligned}$$

Note that for $1 \leq j \leq 4$ and $J \subset \Omega$ we have $\varphi_j(\xi_J) = \pm \epsilon_j$, where the sign is negative if and only if we have $j \in J$. For the evaluation of various linear forms at the intersection points of the lines in Λ , it will also be convenient to notice that we have

$$\sum_{j=1}^4 \omega_j^r \kappa_j^{-1} = \begin{cases} -c_4^{-1} & r = -1, \\ 0 & r = 0, 1, 2, \\ 1 & r = 3. \end{cases} \quad (2)$$

It will turn out that the elliptic fibration associated to \mathcal{S} factors through the projection of $\mathbb{P}(\bar{A})$ to \mathbb{P}^3 by the coordinates φ_i for $1 \leq i \leq 4$, i.e., the projection away from the line given by $\varphi_i = 0$ for $1 \leq i \leq 4$. The image of \bar{V} under this projection is the nonsingular quadric $D_{\omega_5 \omega_6}$ of Remark 2.1.5. Note that \bar{V} is contained in the inverse image of $D_{\omega_5 \omega_6}$ under the indicated projection, which is the cone over the cone over $D_{\omega_5 \omega_6}$ in $\mathbb{P}(\bar{A})$, given by $Q = 0$ with

$$Q = \omega_5 \omega_6 Q_0 - (\omega_5 + \omega_6) Q_1 + Q_2 = \sum_{j=1}^4 \kappa_j^{-1} \delta_j \varphi_j^2, \quad (3)$$

as was pointed out in Remark 2.1.5. Consider the linear forms

$$\begin{aligned} l_1 &= \sum_{j=1}^4 \kappa_j^{-1} \epsilon_j \varphi_j, & m_1 &= \sum_{j=1}^4 \omega_j (2\omega_j - c_1) \kappa_j^{-1} \epsilon_j \varphi_j, \\ l_2 &= \sum_{j=1}^4 \omega_j \kappa_j^{-1} \epsilon_j \varphi_j, & m_2 &= \sum_{j=1}^4 (2c_4 \omega_j^{-1} - c_3) \kappa_j^{-1} \epsilon_j \varphi_j. \end{aligned}$$

Lemma 2.3.1 *On \bar{V} we have $l_1 m_2 = l_2 m_1$. The map $\chi: \bar{V} \rightarrow \mathbb{P}^1$ that sends x to $[l_1(x) : m_1(x)] = [l_2(x) : m_2(x)]$ is an elliptic fibration, defined over $k_g([S])$. The 4-gons S_1, S_2, S_3, S_4 are fibers above $[-1 : \alpha_1]$, $[-1 : \alpha_2]$, $[-1 : \alpha_3]$, and $[0 : 1]$ respectively.*

Proof. From (2) one easily works out that $m_1 l_2 - l_1 m_2 = Q$, so on \bar{V} we find $l_1 m_2 = l_2 m_1$. The four equations $l_1 = m_1 = l_2 = m_2 = 0$ are linearly independent, so the base locus of the map χ is given by $\varphi_i = 0$ on \bar{V} , for $1 \leq i \leq 4$. Together with the equations $Q_0 = Q_1 = Q_2 = 0$ (see Proposition 2.1.2), this implies that the base locus of χ is empty. The fiber F_0 of χ above $[a : b]$ is the intersection of \bar{V} with the three-space given by $bl_i = am_i$ for $i = 1, 2$. The quadric Q vanishes on this three-space, in which the fiber F_0 is therefore given by $Q_0 = Q_1 = 0$. Since every smooth intersection of two quadrics in \mathbb{P}^3 is a curve of genus 1, we deduce that χ is an elliptic fibration, whose fibers all have degree 4. The intersection points of the lines in S_4 are P_{ξ, ω_r} with $\xi \in \{\xi_0, \xi_{56}\}$, and $r \in \{5, 6\}$. From (2) and the identity

$$\epsilon_j \varphi_j (\xi_I^{-1}(X - \omega_r)) = \pm (\omega_j - \omega_r), \quad (4)$$

where the sign is positive if and only if $j \notin I$, we find that the l_i vanish on these points, and thus on the lines in S_4 . This implies that S_4 is contained in the fiber above $[0 : 1]$. Since all fibers have degree 4, the union of the lines in S_4 is a whole fiber. The lines in $S_1 \cup S_2 \cup S_3$ do not intersect any line in S_4 , so they are fibral as well, which implies that all $S \in \mathcal{S}$ are fibers of χ . Their images are easily computed by evaluating the l_i/m_i on the appropriate intersection points P_{ξ, ω_5} of two lines in the 4-gons, using (4) and perhaps a computer algebra package to verify that for instance the ratio $l_1(P_{\xi_{24}, \omega_5}) : m_1(P_{\xi_{24}, \omega_5})$, which is the ratio between

$$\frac{\omega_1 - \omega_5}{\kappa_1} - \frac{\omega_2 - \omega_5}{\kappa_2} + \frac{\omega_3 - \omega_5}{\kappa_3} - \frac{\omega_4 - \omega_5}{\kappa_4}$$

and

$$\frac{\omega_1(2\omega_1 - c_1)(\omega_1 - \omega_5)}{\kappa_1} - \frac{\omega_2(2\omega_2 - c_1)(\omega_2 - \omega_5)}{\kappa_2} + \frac{\omega_3(2\omega_3 - c_1)(\omega_3 - \omega_5)}{\kappa_3} - \frac{\omega_4(2\omega_4 - c_1)(\omega_4 - \omega_5)}{\kappa_4},$$

does indeed equal $-1 : \alpha_2$ (see [21]). Since χ is also given by $[\eta l_i : \eta m_i]$, and the polynomials ηl_i and ηm_i are fixed by $\rho_g^{-1}(G_{[S]})$, we find that χ is defined over $k_g([S])$. \square

Remark 2.3.2 The map χ of Lemma 2.3.1 is in fact defined over $k_g(S_1)$. We found the linear forms l_i and m_i as follows. Using simple linear algebra we found linear forms h_1, h_2, h_3, h_4 vanishing on the lines in $S_4 \cup S_5$, $S_4 \cup S_6$, $S_3 \cup S_5$, and $S_3 \cup S_6$ respectively. The elliptic fibrations given by $[h_1 : h_2]$ and $[h_3 : h_4]$ both have the 4-gons in S' as fibers, so they differ by an automorphism of the base, which fixes the points $[0 : 1]$ and $[1 : 0]$ as both fibrations have the same fibers S_5 and S_6 there. This implies that after the appropriate scaling of the h_i we may assume $h_1 h_4 = h_2 h_3$. The space of linear forms vanishing on S_4 is spanned by h_1 and h_2 . We can pick a $k(S_4)$ -basis $l'_1 = ah_1 + bh_2$ and $l'_2 = ch_1 + dh_2$ for some $a, b, c, d \in m_g$. The fibers F_1 and F_2 of the fibration $[h_1 : h_2] = [h_3 : h_4]$ above the points $[-b : a]$ and $[-d : c]$ respectively are then defined over $k(S_4)$, as they are the complement of S_4 inside the hyperplane section given by l'_1 and l'_2 respectively. The space of linear forms vanishing on F_1 is spanned by l'_1 and $m''_1 = ah_3 + bh_4$. For some p, q , the form $m'_1 = pl'_1 + qm''_1 = pl'_1 + aqh_3 + bqh_4$ is also defined over $k(S_4)$. Set $m'_2 = pl'_2 + cqh_3 + dqh_4$. Then from $h_1 h_4 = h_2 h_3$ we also find $l'_1 m'_2 = l'_2 m'_1$ on \bar{V} . For some choice of a, b, c, d, p, q , the given l_i and m_i satisfy $l'_i = \eta l_i$, and $m'_i = \eta m_i$.

2.3.2 The fibration over a conic

Let $\tau \in \text{Gal}(m_g/k_g)$ denote the automorphism that fixes all the ω_j and the ϵ_j for $j \geq 3$, and sends ϵ_i to $-\epsilon_i$ for $i = 1, 2$. Then τ induces the nontrivial automorphism of the quadratic extension $k_g([S])/n_g(\beta_3)$, generated by β_2 . Since τ permutes the 4-gons in S , the elliptic fibration ${}^\tau\chi$ differs from χ by some automorphism ψ of the base curve \mathbb{P}^1 by Proposition 2.1.26, i.e., we have ${}^\tau\chi = \psi \circ \chi$. This implies that the image of the map $(\chi, {}^\tau\chi) : \bar{V} \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$ is contained in the graph of ψ . Under the Segre embedding $\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^3$ this graph maps to a conic that we can embed in \mathbb{P}^2 . We will now make this explicit. For $i = 1, 2$ we set

$$p_i = 2({}^\tau l_i)l_i, \quad q_i = ({}^\tau l_i)m_i + ({}^\tau m_i)l_i + 2\alpha_3 l_i {}^\tau l_i, \quad r_i = \beta_2^{-1}({}^\tau m_i)l_i - ({}^\tau l_i)m_i.$$

Let $C_1 \subset \mathbb{P}^2$ be the conic given by $\gamma_1 \gamma_2 p^2 + q^2 = \beta_2^2 r^2$.

Lemma 2.3.3 *There is an elliptic fibration $\nu_1 : \bar{V} \rightarrow C_1$, defined over $n_g(\beta_3)$, given by $x \mapsto [p_i(x) : q_i(x) : r_i(x)]$ for $i = 1, 2$, such that the 4-gons S_1, S_2, S_3, S_4 are fibers above $[2 : \gamma_1 - \gamma_2 : -\gamma_3 \beta_2^{-1}]$, $[2 : \gamma_1 - \gamma_2 : \gamma_3 \beta_2^{-1}]$, $[0 : \beta_2 : 1]$, and $[0 : \beta_2 : -1]$ respectively.*

Proof. Note that the images of the S_i under χ , given in Lemma 2.3.1, are τ -invariant. This implies $({}^\tau\chi)(S_i) = {}^\tau(\chi({}^{\tau^{-1}}S_i)) = \chi({}^\tau S_i)$. Note also that τ acts on the S_i as the permutation $(S_1 S_2)(S_3 S_4)$. By Proposition 2.1.26 the elliptic fibrations ${}^\tau\chi$ and χ differ by an automorphism of \mathbb{P}^1 . As an automorphism of \mathbb{P}^1 is determined by its action on the $\chi(S_i)$, this allows us to check that the automorphism $\psi : [s : t] \mapsto [-\alpha_3 s - t : (\alpha_3^2 + \gamma_1 \gamma_2)s + \alpha_3 t]$ of \mathbb{P}^1 satisfies ${}^\tau\chi = \psi\chi$. By Lemma 2.3.1 it suffices to check that ψ switches the points $[-1 : \alpha_1]$ and $[-1 : \alpha_2]$ and also the points $[-1 : \alpha_3]$ and $[0 : 1]$ (see [21]). We conclude that $(\chi, {}^\tau\chi) : \bar{V} \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$ is an elliptic fibration over the graph of ψ .

Let $h : \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^3$ denote the modified Segre embedding that sends $([a : b], [c : d])$ to $[x : y : z : w] = [ac : ad + bc : \beta_2^{-1}(ad - bc) : bd]$. Then the composition $g = h \circ (\chi, {}^\tau\chi) : \bar{V} \rightarrow \mathbb{P}^3$ is τ -invariant, so it is defined over $n_g(\beta_3)$. The image of the graph of ψ under h is the conic given by $y^2 - \beta_2^2 z^2 = 4xw$ and $(\alpha_3^2 + \gamma_1 \gamma_2)x + \alpha_3 y + w = 0$. The image of this conic under the projection $\pi : \mathbb{P}^3 \rightarrow \mathbb{P}^2, [x, y, z, w] \mapsto [2x : y + 2\alpha_3 x : z]$ is C_1 , so the composition $\nu_1 = \pi \circ g$ is an elliptic fibration of \bar{V} over C_1 . Since π and g are defined over $n_g(\beta_3)$, so is ν_1 . As χ is given by $[l_i : m_i]$, for $i = 1, 2$, one checks easily that the fibration ν_1 is given by $[p_i : q_i : r_i]$. The images of the fibers are easily computed using the images given in Lemma 2.3.1 and the fact that we have $({}^\tau(l_i/m_i))(S_i) = (l_i/m_i)({}^\tau S_i)$ as noted above. \square

We will construct an automorphism ψ of \mathbb{P}^2 such that $\psi \circ \nu_1$ is an elliptic fibration from \bar{V} to a conic C , such that both C and the fibration are defined over $k_g(S)$, the field of definition of the fibration. We know that there is an elliptic fibration over a conic defined over $k_g(S)$ whose fibers include the 4-gons of S . By Proposition 2.1.26 it is unique up to an isomorphism of the conic, so we know such a ψ exists. We will do this in two steps by first descending to n_g and then to $k_g(S)$. Suppose at some step we have a fibration $\nu_i : \bar{V} \rightarrow C_i$, with C_i a conic, defined over a field K_i that is Galois over K_{i+1} with Galois group G_i . We are

looking for an automorphism ψ_i of \mathbb{P}^2 such that $\nu_{i+1} = \psi_i \circ \nu_i: \bar{V} \rightarrow C_{i+1}$ with $C_{i+1} = \psi_i(C_i)$ is defined over K_{i+1} .

For all $g \in G_i$ there is an isomorphism $\sigma(g): {}^g C_i \rightarrow C_i$ such that $\nu_i = \sigma(g) \circ {}^g \nu_i$. Since $\sigma(g)^*: \text{Pic } C_i \rightarrow \text{Pic } {}^g C_i$ sends the canonical divisor of C_i to that of ${}^g C_i$, the automorphism $\sigma(g)$ is induced by a unique automorphism of \mathbb{P}^2 , which we will also denote by $\sigma(g)$. These automorphisms satisfy the cocycle condition $\sigma(hg) = \sigma(h) \circ {}^h \sigma(g)$. The automorphism ψ_i that we seek satisfies $\psi_i \circ \sigma(g) = {}^g \psi_i$, so σ is a coboundary with values in $\text{Aut } \mathbb{P}_{K_i}^2$.

$$\begin{array}{ccccc}
 & & {}^g C_i & & \\
 & \nearrow {}^g \nu_i & \downarrow \sigma(g) & \searrow {}^g \psi_i & \\
 \bar{V} & \xrightarrow{\nu_{i+1}} & C_{i+1} & & \\
 & \searrow \nu_i & \downarrow \psi_i & & \\
 & & C_i & &
 \end{array}$$

We can find ψ_i as follows. Consider the homomorphism $\text{GL}_3(K_i) \rightarrow \text{Aut } \mathbb{P}_{K_i}^2$ that maps a matrix $M \in \text{GL}_3(K_i)$ to the automorphism that sends $[x : y : z]$ to $[x' : y' : z']$ with $(x' y' z')^t = M(x y z)^t$. Through this homomorphism we may identify $\text{Aut } \mathbb{P}_{K_i}^2$ with $\text{PGL}_3(K_i)$.

Our first step will be to lift σ to a cocycle for $\text{GL}_3(K_i)$. The map $\det: \text{GL}_3(K_i) \rightarrow K_i^*$, $M \mapsto \det(M)$ induces a homomorphism $\text{PGL}_3(K_i) \rightarrow K_i^*/K_i^{*3}$. For any G_i -set M , let $Z^1(M)$ denote the corresponding set of 1-cocycles with coefficients in M . We obtain the following diagram.

$$\begin{array}{ccccccc}
 & 1 & & 1 & & 1 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 1 & \longrightarrow & Z^1(\mu_3(K_i)) & \longrightarrow & Z^1(\text{SL}_3(K_i)) & \longrightarrow & Z^1(\text{PSL}_3(K_i)) \longrightarrow H^2(\mu_3(K_i)) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & Z^1(K_i^*) & \longrightarrow & Z^1(\text{GL}_3(K_i)) & \longrightarrow & Z^1(\text{PGL}_3(K_i)) \longrightarrow H^2(K_i^*) \\
 & & \downarrow [3] & & \downarrow \det & & \downarrow \det \\
 1 & \longrightarrow & Z^1(K_i^{*3}) & \longrightarrow & Z^1(K_i^*) & \longrightarrow & Z^1(K_i^*/K_i^{*3}) \longrightarrow H^2(K_i^{*3})
 \end{array}$$

Since $\sigma \in Z^1(\text{PGL}_3(K_i))$ is in fact a coboundary, it maps to zero in $H^1(\text{PGL}_3(K_i))$, so it also maps to zero in $H^2(K_i^*)$. Therefore we can lift σ to an element $\sigma' \in Z^1(\text{GL}_3(K_i))$. To do this in practice we note that we are working over a generic field, so we may assume K_i has no cube roots of unity. This implies that $\text{SL}_3(K_i)$ is isomorphic to the subgroup $\text{PSL}_3(K_i)$ of $\text{PGL}_3(K_i)$, so an element $M \in \text{GL}_3(K_i)$ is uniquely determined by its determinant and its image in $\text{PGL}_3(K_i)$. Thus $\sigma' \in Z^1(\text{GL}_3(K_i))$ is uniquely determined by its image σ and $\det \sigma' \in Z^1(K_i^*)$, which is a lift of $\det \sigma \in Z^1(K_i^*/K_i^{*3})$. To find σ' it therefore suffices to find a lift of $\det \sigma \in Z^1(K_i^*/K_i^{*3})$ to $Z^1(K_i^*)$. In our case $\det \sigma$ will always be trivial, so this step is easy.

The second step is to write $\sigma' = Z^1(\text{GL}_3(K_i))$ as a coboundary, which is possible as we have $H^1(\text{GL}_3(K_i)) = 1$ by a generalization of Hilbert 90. For this we use a standard trick, discussed in [16], Proposition X.3. For any matrix M we set

$$b_M = \sum_{g \in G} \sigma'(g)({}^g M).$$

One checks that we have $\sigma'(h) \cdot {}^h b_M = b_M$. Choosing M carefully so that b_M is invertible, we may take ψ_i to be the automorphism associated to the matrix b_M^{-1} . After some simplifications of these automorphisms we get the following lemma, which can in fact be checked without knowing how we obtained the equations.

Let $C_2 \subset \mathbb{P}^2(u, v, w)$ be the conic given by $\gamma_1\beta_1^2u^2 + \gamma_2\beta_2^2v^2 + \gamma_3\beta_3^2w^2$ and set

$$\begin{aligned} u_i &= \beta_1^{-1}(q_i + \gamma_2 p_i) = \beta_1^{-1}(\tau_l m_i + \tau_{m_i} l_i + 2\alpha_1 l_i \tau_l), \\ v_i &= \beta_2^{-1}(q_i - \gamma_1 p_i) = \beta_2^{-1}(\tau_l m_i + \tau_{m_i} l_i + 2\alpha_2 l_i \tau_l), \\ w_i &= -\beta_2\beta_3^{-1}r_i = \beta_3^{-1}(\tau_l m_i - \tau_{m_i} l_i). \end{aligned}$$

Lemma 2.3.4 *There is an elliptic fibration $\nu_2: \bar{V} \rightarrow C_2$, defined over n_g , given by $x \mapsto [u_i(x) : v_i(x) : w_i(x)]$ for $i = 1, 2$, such that the 4-gons S_1, S_2, S_3, S_4 are fibers above $[-\beta_1^{-1} : \beta_2^{-1} : \beta_3^{-1}]$, $[\beta_1^{-1} : -\beta_2^{-1} : \beta_3^{-1}]$, $[\beta_1^{-1} : \beta_2^{-1} : -\beta_3^{-1}]$, and $[\beta_1^{-1} : \beta_2^{-1} : \beta_3^{-1}]$ respectively.*

Proof. The nontrivial automorphism π of the extension $n_g(\beta_3)/n_g$ is induced by the automorphism that fixes all ω_j and all ϵ_j , except for ϵ_1 and ϵ_3 , which are sent to their negatives. It acts on the S_i as the permutation $(S_1 S_3)(S_2 S_4)$. The composition $\nu_2: \bar{V} \rightarrow \mathbb{P}^2$ of ν_1 and

$$\psi: \mathbb{P}^2 \rightarrow \mathbb{P}^2, [p : q : r] \mapsto [\beta_1^{-1}(q + \gamma_2 p) : \beta_2^{-1}(q - \gamma_1 p) : -\beta_2\beta_3^{-1}r]$$

is given by $x \mapsto [u_i(x) : v_i(x) : w_i(x)]$. The inverse of ψ is given by

$$[u : v : w] \mapsto [\beta_1 u - \beta_2 v : \gamma_1 \beta_1 u + \gamma_2 \beta_2 v : \gamma_3 \beta_2^{-1} \beta_3 w].$$

Substituting this into the equation for C_1 , we find that the conic $\psi(C_1)$ is equal to C_2 . Alternatively, one checks that we have

$$\gamma_1\beta_1^2u_i^2 + \gamma_2\beta_2^2v_i^2 + \gamma_3\beta_3^2w_i^2 = 4\gamma_3b_i\tau_l l_i Q,$$

with $b_1 = \omega_1 + \omega_2 - \omega_3 - \omega_4$ and $b_2 = -c_4(\omega_1^{-1} + \omega_2^{-1} - \omega_3^{-1} - \omega_4^{-1})$ (see [21]). Since Q vanishes on V , this also shows that ν_2 maps \bar{V} to C_2 . As π permutes \mathcal{S} , the 4-gons in \mathcal{S} are also fibers of $\pi\nu_2$, so ν_2 and $\pi\nu_2$ differ by an isomorphism on the base by Proposition 2.1.26. Therefore, there is a unique isomorphism $h: C_2 \rightarrow \pi C_2 = C_2$ such that $\pi\nu_2 = h \circ \nu_2$. Since h fixes the anticanonical divisor on C_2 , which determines the embedding of C_2 in \mathbb{P}^2 , the isomorphism h comes from a unique automorphism of \mathbb{P}^2 , which we will also denote by h . With the points $\nu_1(S_i)$ given in Lemma 2.3.3, one easily computes $\nu_2(S_i) = \psi(\nu_1(S_i))$ to be as claimed. With the identity $(\pi\nu_2)(S_i) = \pi(\nu_2(\pi^{-1}S_i))$ we check that we have $(\pi\nu_2)(S_i) = \nu_2(S_i)$ for $1 \leq i \leq 4$, so h fixes the four points $\nu_2(S_i)$. As these points all lie on C_2 , no three of them are collinear. This implies that the action of h on the four points determines h uniquely, which means that h is the identity, so $\pi\nu_2 = \nu_2$. We conclude that ν_2 is defined over the fixed field n_g of π . \square

Finally, we let $C_3 \subset \mathbb{P}^2(x, y, z)$ be the conic given by

$$\gamma_1\beta_1^2(x + \gamma_1\Delta_4y + (\alpha_2 + \alpha_3)z)^2 + \gamma_2\beta_2^2(x + \gamma_2\Delta_4y + (\alpha_1 + \alpha_3)z)^2 + \gamma_3\beta_3^2(x + \gamma_3\Delta_4y + (\alpha_1 + \alpha_2)z)^2 = 0,$$

and we set

$$\begin{aligned} x_i &= 2\Delta_4((\alpha_2\alpha_3 - \alpha_1^2)u_i + (\alpha_1\alpha_3 - \alpha_2^2)v_i + (\alpha_1\alpha_2 - \alpha_3^2)w_i), \\ y_i &= -\gamma_1u_i - \gamma_2v_i - \gamma_3w_i, \\ z_i &= \Delta_4((\gamma_2 - \gamma_3)u_i + (\gamma_3 - \gamma_1)v_i + (\gamma_1 - \gamma_2)w_i). \end{aligned}$$

Lemma 2.3.5 *There is an elliptic fibration $\nu_3: \bar{V} \rightarrow C_3$, defined over $k_g(\mathcal{S})$, given by $x \mapsto [x_i(x) : y_i(x) : z_i(x)]$ for $i = 1, 2$, such that the 4-gons of \mathcal{S} are fibers of ν_3 .*

Proof. Let $\pi_1, \pi_2 \in \text{Gal}(n_g/k_g(\mathcal{S}))$ denote the automorphisms induced by the permutations $(\omega_1 \omega_2 \omega_3)$ and $(\omega_1 \omega_2)$ on the ω_j respectively and the corresponding permutation on the ϵ_j . Then π_1 and π_2 induce generators of $\text{Gal}(n_g/k_g(\mathcal{S}))$. They act on \mathcal{S} , the $\alpha_j, \beta_j, \gamma_j$, and the ϕ_j as the permutations $(1 \ 2 \ 3)$ and $(1 \ 2)$

on the indices, except that π_2 also negates the γ_j . Note also that we have $\pi_1(\Delta_4) = \Delta_4$ and $\pi_2(\Delta_4) = -\Delta_4$. The composition $\nu_3: \bar{V} \rightarrow \mathbb{P}^2$ of ν_2 and $\psi: \mathbb{P}^2 \rightarrow \mathbb{P}^2$, $[u : v : w] \mapsto [x : y : z]$ with

$$\begin{aligned} x &= 2\Delta_4((\alpha_2\alpha_3 - \alpha_1^2)u + (\alpha_1\alpha_3 - \alpha_2^2)v + (\alpha_1\alpha_2 - \alpha_3^2)w), \\ y &= -\gamma_1u - \gamma_2v - \gamma_3w, \\ z &= \Delta_4((\gamma_2 - \gamma_3)u + (\gamma_3 - \gamma_1)v + (\gamma_1 - \gamma_2)w). \end{aligned}$$

is given by $P \mapsto [x_i(P) : y_i(P) : z_i(P)]$. The inverse of ψ is given by

$$[x : y : z] \mapsto [x + \gamma_1\Delta_4y + (\alpha_2 + \alpha_3)z : x + \gamma_2\Delta_4y + (\alpha_1 + \alpha_3)z : x + \gamma_3\Delta_4y + (\alpha_1 + \alpha_2)z].$$

Substituting this in the equation for C_2 , we find that the conic $\psi(C_2)$ is equal to C_3 , so ν_3 maps \bar{V} to C_3 . Note that for all $g \in \text{Gal}(n_g/k_g(\mathcal{S}))$ we have ${}^gC_3 = C_3$. As in the proof of Lemma 2.3.4, for all $g \in \text{Gal}(n_g/k_g(\mathcal{S}))$ there is an automorphism h_g of \mathbb{P}^2 such that we have ${}^g\nu_3 = h_g \circ \nu_3$. Evaluating ψ at the points $\nu_2(S_i)$ given in Lemma 2.3.4 and using the identity $({}^g\nu_3)(S_i) = {}^g(\psi(\nu_2({}^{g^{-1}}S_i)))$, we check that for all $g \in \text{Gal}(n_g/k_g(\mathcal{S}))$ we have $({}^g\nu_3)(S_i) = \nu_3(S_i)$ for $1 \leq i \leq 4$. It suffices to check this for $g = \pi_1, \pi_2$. As in the proof of Lemma 2.3.4 this implies that for all $g \in \text{Gal}(n_g/k_g(\mathcal{S}))$ the automorphism h_g is the identity, so ${}^g\nu_3 = \nu_3$. We conclude that ν_3 is defined over $k_g(\mathcal{S})$. \square

Remark 2.3.6 Even though the fibration ν_3 is defined over $k_g(\mathcal{S})$, the polynomials x_i, y_i, z_i that describe ν_3 are not, and neither is the defining equation of C_3 . The latter issue is easily resolved by multiplying the given equation for C_3 by Δ_4 to obtain an equation defined over $k(\mathcal{S})$. To settle the former, we can replace x_i, y_i, z_i with Galois-invariant polynomials as follows. Again we descend from the field $k_g([\mathcal{S}])$ to $k_g(\mathcal{S})$ in steps. The polynomials l_i and m_i are not defined over $k_g([\mathcal{S}])$, but ηl_i and ηm_i are, as they are fixed by the elements of $G_{[\mathcal{S}]}$, see Lemma 2.2.14. Scaling by $\beta_2{}^\tau\eta\eta$, we find that the polynomials $u'_i = \beta_2{}^\tau\eta\eta u_i$, $v'_i = \beta_2{}^\tau\eta\eta v_i$, and $w'_i = \beta_2{}^\tau\eta\eta w_i$ are also defined over $n_g(\beta_3)$ and define ν_2 as well. Since ν_2 is defined over n_g , the polynomials ${}^\pi u'_i, {}^\pi v'_i$, and ${}^\pi w'_i$, define ν_2 as well, where π is the nontrivial automorphism of $n_g(\beta_3)/n_g$ as in the proof of Lemma 2.3.4. This implies that ν_2 can also be defined by $[u''_i : v''_i : w''_i]$ with $u''_i = u'_i + {}^\pi u'_i$, $v''_i = v'_i + {}^\pi v'_i$, and $w''_i = w'_i + {}^\pi w'_i$ unless these polynomials vanish on V , which they turn out not to. One checks for instance that we have

$$\begin{aligned} \frac{\beta_1 u''_1}{\beta_2} &= 8(\epsilon_1\epsilon_2 - \epsilon_3\epsilon_4) \left(\frac{\kappa_1^{-1}\delta_1\varphi_1^2 + \kappa_4^{-1}\delta_4\varphi_4^2}{\omega_1 - \omega_4} + \frac{\kappa_2^{-1}\delta_2\varphi_2^2 + \kappa_3^{-1}\delta_3\varphi_3^2}{\omega_2 - \omega_3} \right) \\ &\quad + 4(\delta_1 + \delta_2 - \delta_3 - \delta_4)(\omega_1 - \omega_2 - \omega_3 + \omega_4) ((\omega_1 - \omega_2)\kappa_1^{-1}\kappa_2^{-1}\epsilon_1\epsilon_2\varphi_1\varphi_2 + (\omega_3 - \omega_4)\kappa_3^{-1}\kappa_4^{-1}\epsilon_3\epsilon_4\varphi_3\varphi_4) \end{aligned}$$

(see [21]). With the same trick we descend to $k_g(\mathcal{S})$. The polynomials

$$\begin{aligned} x'_i &= 2\Delta_4((\alpha_2\alpha_3 - \alpha_1^2)u''_i + (\alpha_1\alpha_3 - \alpha_2^2)v''_i + (\alpha_1\alpha_2 - \alpha_3^2)w''_i), \\ y'_i &= -\gamma_1u''_i - \gamma_2v''_i - \gamma_3w''_i, \\ z'_i &= \Delta_4((\gamma_2 - \gamma_3)u''_i + (\gamma_3 - \gamma_1)v''_i + (\gamma_1 - \gamma_2)w''_i). \end{aligned}$$

are defined over n_g and ν_3 is defined by $[x'_i : y'_i : z'_i]$. Since ν_3 is defined over $k_g(\mathcal{S})$, it is also defined by $[{}^g x'_i : {}^g y'_i : {}^g z'_i]$ for any $g \in \text{Gal}(n_g/k_g(\mathcal{S}))$ and therefore by $[x''_i : y''_i : z''_i]$ with $x''_i = \sum_{g \in \text{Gal}(n_g/k_g(\mathcal{S}))} {}^g x'_i$, $y''_i = \sum_{g \in \text{Gal}(n_g/k_g(\mathcal{S}))} {}^g y'_i$, and $z''_i = \sum_{g \in \text{Gal}(n_g/k_g(\mathcal{S}))} {}^g z'_i$, unless these polynomials, defined over $k(\mathcal{S})$, vanish on V . An explicit computation shows that they do not. Over $k_g(\mathcal{S})$ we can write $f = f_2 f_4$ with $f_4 = X^4 - c_1 X^3 + c_2 X^2 - c_3 X + c_4$, where the c_r are the symmetric polynomials in the ω_j ($1 \leq j \leq 4$) of degree r . The image in $A_4 = k_g[X]/f_4$ of $\delta \in A$ can be written as $\delta' = d_3 X^3 + d_2 X^2 + d_1 X + d_0$ with $d_i \in k_g(c_1, c_2, c_3, c_4)$. We may also consider the d_i to be independent transcendentals contained in k_g (here the d_i are not the same as in Example 2.2.10). Let N denote a square root of the norm $N_{A_4/k_g}(\delta')$ of δ' . Note that as always we have $\varphi_j = \sum_{i=0}^5 \omega_j^i a_i$, where the a_i are the original coordinates of $\mathbb{P}(A)$. The polynomials x''_i, y''_i , and z''_i are quadratic in the a_i with coefficients in the field $\mathbb{Q}(c_1, c_2, c_3, c_4, d_0, d_1, d_2, d_3, N)$. Expressing

them as such takes a file that has size about one megabyte [21]. Note also that the equations for the fibration do not depend on ω_5 and ω_6 . This shows that the fibration does indeed factor through the quadric $D_{\omega_5\omega_6}$ in \mathbb{P}^3 of Remark 2.1.5, because that is the image of \bar{V} under the projection from $\mathbb{P}(\bar{A})$ to \mathbb{P}^3 using only the coordinates $\varphi_1, \dots, \varphi_4$.

Remark 2.3.7 In any specific example, we can consider the specialization of the equations for C_3 and the fibration ν_3 in Lemma 2.3.5, or better, Remark 2.3.6. For a proper closed subset in the family of all curves of genus 2 and choices of δ these equations may vanish. Outside this subset, this specialization gives us an elliptic fibration ν of a surface V over a conic C . If V is everywhere locally solvable, then so is C . Since C satisfies the Hasse principle, this implies that C has a rational point, which can be found by standard algorithms. This gives us a rational fiber F_0 on V . The linear system of hyperplanes through F_0 is 2-dimensional and determines an elliptic fibration ν' of V over \mathbb{P}^1 , given by linear polynomials. The 4-gons that are fibers of ν' belong to the complementary exhibit of the exhibit whose 4-gons are fibers of ν . Applying the same trick again, we also obtain an elliptic fibration over \mathbb{P}^1 that is equivalent to ν . On the other hand, even if C is everywhere locally solvable, V may not be.

3 Arithmetical applications

In this section we apply the theory of the previous sections, combined with the idea of the Brauer-Manin obstruction, to give an example of a K3 surface arising from 2-descent on a family of curves of genus 2 that has rational points everywhere locally but not globally, and hence a family of curves of genus 2 all having nontrivial Tate-Shafarevich group.

3.1 The Brauer group and the Brauer-Manin obstruction

To explain the Brauer-Manin obstruction, let V be a variety over a number field K . If there is a place \mathfrak{p} of K at which V has no points, then of course V has no K -rational points. But if V has points everywhere locally, we can sometimes use the Brauer group to prove that it does not have any points defined over K . We begin by defining the Brauer group of a scheme; this material is taken from the beginning of [12], chapter 4.

Definition 3.1.1 *Let R be a ring. Then an Azumaya algebra A over R is a free R -algebra of finite rank as an R -module such that $A \otimes_R A^{\text{op}}$ is isomorphic to $\text{End}(A)$ by the map taking $a \otimes a'$ to the endomorphism $x \rightarrow axa'$.*

Definition 3.1.2 *Let V be a scheme. An Azumaya algebra \mathcal{A} on V is a coherent sheaf of R -algebras whose stalk at every point x of V is an Azumaya algebra over the local ring of V at x . The Brauer group of V is the semigroup of Azumaya algebras on V under tensor product modulo the subsemigroup of endomorphism algebras of locally free sheaves.*

The Brauer group of a field K is often defined as the semigroup of finite-dimensional central simple algebras over K under the operation of tensor product modulo the subsemigroup $\{M_n(K) : n \in \mathbb{N}\}$. This is a special case of the definition above. Alternatively, $\text{Br } K$ can be thought of as $H^2(K, K^{\text{sep}*})$, which can be rewritten as $H_{\text{ét}}^2(\text{Spec } K, K^{\text{sep}*})$ using the standard equivalence ([12], Example III.1.7) between étale cohomology of $\text{Spec } K$ and Galois cohomology of $\text{Gal}(K^{\text{sep}}/K)$ -modules. We extend this definition to general schemes as follows.

Definition 3.1.3 *For a variety V over a field K , we use \bar{V} to denote $V \otimes_K \bar{K}$.*

Definition 3.1.4 *The cohomological Brauer group $\text{Br } V$ of a scheme V is $H_{\text{ét}}^2(V, \mathbb{G}_m)$. If V is defined over a field K , then the algebraic part of the Brauer group $\text{Br}_1 V$ is the kernel of the natural map $\text{Br } V \rightarrow \text{Br } \bar{V}$.*

We can use the Brauer group to find obstructions to the existence of points, but it is difficult to compute. However, we can compute the algebraic part of the Brauer group. By [12], Prop. IV.2.15, the Brauer group and the cohomological Brauer group are isomorphic when V is a smooth variety over a field. For V defined over a number field, the algebraic part of the Brauer group can be computed as $H^1(K, \text{Pic } \bar{V})$, as shown in [4], sect. 4.1. As stated in Corollary 2.1.4, we have $\text{Pic } \bar{V} = \text{NS } \bar{V}$, a finitely generated free abelian group.

In this paper, we will only consider the algebraic part of the Brauer group. Now we explain how to use the Brauer group to show that V has no K -rational points.

Definition 3.1.5 *Let K be a number field and \mathfrak{p} a place of K . The local invariant $\text{inv}_{\mathfrak{p}}(s)$ of an element s of the Brauer group of the local field $K_{\mathfrak{p}}$ is its image under the natural homomorphism $\text{Br } K_{\mathfrak{p}} \rightarrow \mathbb{Q}/\mathbb{Z}$ ([16], Proposition XII.6).*

Recall that this homomorphism is always injective, and that it is surjective if \mathfrak{p} is non-archimedean, while its image is generated by $1/2$ if \mathfrak{p} is real and is trivial if \mathfrak{p} is complex.

Definition 3.1.6 For $s \in \text{Br } V$, \mathfrak{p} a place of K , and $P \in V(K_{\mathfrak{p}})$, the local invariant of s at P is the local invariant $\text{inv}_{\mathfrak{p}}(s_P)$ of the element $s_P \in \text{Br } K_{\mathfrak{p}}$ obtained by pulling back the cohomology class s by the map $\text{Spec } K_{\mathfrak{p}} \rightarrow V$ whose image is the point P . More concretely, it is the local invariant of the Azumaya algebra over $K_{\mathfrak{p}}$ whose multiplication table is given by evaluating the elements of the multiplication table of an Azumaya algebra representing s at the coordinates of P .

Every K -point P of V corresponds to a morphism $\text{Spec } K \rightarrow V$ that induces a map $\text{Br } V \rightarrow \text{Br } K$ by pulling back cohomology. We denote the image of an element $s \in \text{Br } V$ under this map by $s(P)$, yielding a map $V(K) \rightarrow \text{Br } K$ that is also denoted by s . Similarly for every place \mathfrak{p} (archimedean or non-archimedean) of K we get a map $s_{\mathfrak{p}}: V(K_{\mathfrak{p}}) \rightarrow \text{Br } K_{\mathfrak{p}}$. We obtain the following commutative diagram, where the top horizontal map is the diagonal embedding and λ_s is defined to be the composition shown.

$$\begin{array}{ccccc}
V(K) & \xrightarrow{\quad} & \prod_{\mathfrak{p}} V(K_{\mathfrak{p}}) & & \\
\downarrow s & & \downarrow \prod_{\mathfrak{p}} s_{\mathfrak{p}} & \searrow \lambda_s & \\
\text{Br } K & \xrightarrow{\quad} & \bigoplus_v \text{Br } K_{\mathfrak{p}} & \xrightarrow{\sum \text{inv}_{\mathfrak{p}}} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

The bottom row is exact by class field theory, so the image of the top horizontal map is contained in $\lambda_s^{-1}(0)$. If we show that $\bigcap_{s \in \text{Br } V} \lambda_s^{-1}(0) = \emptyset$, then we may conclude that there is no K -rational point on V , and we say that *the Brauer-Manin obstruction blocks the existence of rational points on V* . It suffices to let s run over a set of generators of $\text{Br } V / \text{Br } K$. Often it is more convenient to consider only elements of $\text{Br } V / \text{Br } K$ belonging to a subset B , and then we speak of the Brauer-Manin obstruction on B blocking the existence of rational points.

Proposition 3.1.7 *Let B be a subgroup of $\text{Br } V / \text{Br } K$ of order 2 generated by the element s . Then the Brauer-Manin obstruction on B blocks the existence of rational points on V if and only if, for all \mathfrak{p} , the local invariant of s is constant on $K_{\mathfrak{p}}$ -points of V and the constants do not add to 0.*

Proof. The sufficiency of this condition is clear. For the necessity, note that, if the local invariant is not constant on $K_{\mathfrak{p}}$ -points for some \mathfrak{p} , we may choose an arbitrary collection of local points at other places with invariants adding to $\alpha \in \{0, 1/2\}$ and then choose a $K_{\mathfrak{p}}$ -point whose invariant is equal to α , thus obtaining a system of points with local invariants adding to 0. In the case where the local invariant is constant on $K_{\mathfrak{p}}$ -points for all \mathfrak{p} , the necessity of the condition that the constants not add to 0 is obvious. \square

Now let us explain how to construct K3 surfaces with elements of the Brauer group that are likely to give nontrivial obstructions. Although it is usually easy to calculate $H^1(K, \text{Pic } \bar{V})$, at least when $H^1(V, \mathcal{O}_V) = 0$ and so $\text{Pic } \bar{V}$ is finitely generated, it is difficult to find Azumaya algebras corresponding to nontrivial cohomology classes. Doing so requires finding rational divisors in rational divisor classes. Such divisors always exist if V has points everywhere locally, but in practice it is not easy to find them. Over an algebraically closed field the effective divisors in a linear equivalence class constitute a \mathbb{P}^n , so the problem reduces to finding a rational point on a locally solvable Brauer-Severi variety. This can be reduced to solving a norm equation from a field over which all elements of $\text{Pic } \bar{V}$ are defined, but even when the splitting field of f is fairly small this is likely to be impractical.

We will follow [4], section 4.4, in using elliptic fibrations on varieties to construct nontrivial elements of the Brauer group. For a variety with a fibration ϕ , we define the *vertical Picard group* $\text{Pic}_{\phi} \bar{V}$ to be the subgroup of $\text{Pic } \bar{V}$ spanned by the classes of components of fibers. The *vertical Brauer group* $\text{Br}_{\phi} V$ can then be defined as $H^1(K, \text{Pic}_{\phi} \bar{V})$. (We deviate from the standard notations Pic_{vert} and Br_{vert} used in [4] because it is necessary for us to distinguish between vertical Picard and Brauer groups coming from different fibrations on the same variety.) The inclusion of $\text{Pic}_{\phi} \bar{V}$ into $\text{Pic } \bar{V}$ gives a natural map $\text{Br}_{\phi} V \rightarrow H^1(K, \text{Pic } \bar{V})$, which need not be either injective nor surjective.

It is shown in [4], Prop. 4.21, that elements of $\text{Br}_\phi V$ are represented by Azumaya algebras that are pulled back from central simple algebras on the function field of the target of ϕ . The stalk of such an Azumaya algebra is constant on all fibers of ϕ , so the local invariants of such algebras are too.

Definition 3.1.8 *Let F be any field, and a and b nonzero elements of F . The symbol (a, b) denotes the central simple F -algebra of rank 4 with basis $1, i, j, k$ and multiplication given by $i^2 = a, j^2 = b, ij = k, ji = -k$.*

Proposition 3.1.9 *If F is a local field, the local invariant of (a, b) is 0 if and only if the quadratic form $x^2 - ay^2 - bz^2$ represents 0 nontrivially in F ; otherwise it is $1/2$. In particular, if the residue characteristic of F is odd, then the invariant is 0 if and only if at least one of the following conditions holds: a and b both have even valuation; one of a and b is a square; or ab is a square.*

Proof. The first statement is well-known (note in particular that if a or b is a square then the local invariant is 0). The second follows from the discussion at the beginning of [16], section XIV.4, which applies just as well to any finite extension of \mathbb{Q}_p as to \mathbb{Q}_p itself. \square

Proposition 3.1.10 *Let $\phi : V \rightarrow \mathbb{P}^1$ be an elliptic fibration, and suppose that V has bad fibers of type I_4 over $(\alpha : 1)$, where $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Suppose further that the field of definition of the components of the fiber at $(\alpha : 1)$ is $\mathbb{Q}(\alpha, \sqrt{c})$, where $c \in \mathbb{Q}(\alpha)$ is of square norm, and that the $\mathbb{Q}(\alpha)$ -components of this fiber consist of two disjoint lines. Then the pullback of the algebra $\text{cores}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(c, t - \alpha) \in \text{Br } \mathbb{Q}(t)$ to V , where t is the coordinate on the standard affine patch of \mathbb{P}^1 , is an element of $\text{Br}_\phi V$.*

Proof. This follows immediately from [4], Proposition 4.28. \square

Remark 3.1.11 Note that the hypotheses entail that the fiber consists of two pairs of disjoint lines L_1, M_1 and L_2, M_2 , where all the L_i and M_i are defined and conjugate over one and the same quadratic extension $\mathbb{Q}(\alpha, \sqrt{c})$ of $\mathbb{Q}(\alpha)$.

For this to be useful to us, we need to know how to compute the local invariants of the algebra $\text{cores}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(c, t - \alpha) \in \text{Br } \mathbb{Q}$. The following proposition addresses this question.

Proposition 3.1.12 ([5], Lemma 5 (i)) *The local invariant of $\text{cores}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(c, t - \alpha)$ at p is the sum of those of $(c, t - \alpha)$ at places of $\mathbb{Q}(\alpha)$ lying above p .*

Now we are ready to show how we chose f and δ so that there would be a nontrivial element of the Brauer group arising from an elliptic fibration.

Definition 3.1.13 *From now on, f will always denote a polynomial which is the product of three irreducible quadratic polynomials f_1, f_2, f_3 and δ will be an element of $(\mathbb{Q}[X]/(f))^*$. For given f and δ , let ι be an isomorphism from $\mathbb{Q}[X]/(f)$ to $\oplus_{i=1}^3 \mathbb{Q}[X]/(f_i)$ (which exists by the Chinese Remainder Theorem), fix isomorphisms κ_i from $\mathbb{Q}[X]/(f_i)$ to $\mathbb{Q} \oplus \mathbb{Q}$ (again by the Chinese Remainder Theorem), let v_i be the component of $\iota(\delta)$ in $\mathbb{Q}[X]/(f_i)$, and let v_{ik} be the k th component of $\kappa_i(v_i)$. For convenience define δ_j so that $\delta_{2(i-1)+k} = v_{ik}$ (this notation coincides with the δ_j of Example 2.2.10). Also let σ_i be the nontrivial automorphism of $\mathbb{Q}[X]/(f_i)$ and let r_i be a fixed root of f_i in $\bar{\mathbb{Q}}$.*

Theorem 3.1.14 *With f and δ as above, let V be the K3 surface constructed from f, δ . Suppose further that the splitting field of f is of degree 8; that the norm of v_1 is a square; that the norms of v_2 and v_3 multiplied by the discriminant of f_1 are squares; and that the v_i are otherwise generic. Then the field of definition of the lines of V has degree 32, both elliptic fibrations associated to the factorization $f = (f_1)(f_2 f_3)$ in Remark 2.2.6 satisfy the conditions of Proposition 3.1.10, and the elements of the respective vertical Brauer groups constructed in that proposition map to the same element of $H^1(\mathbb{Q}, \text{Pic } \bar{V})$ and hence to the same element of $\text{Br } V / \text{Br } K$.*

Proof. The condition on δ shows that the norm of the projection of δ to $\mathbb{Q}[X]/(f_2 f_3)$ is a square, so the elliptic fibrations are defined over \mathbb{Q} by Remark 2.2.6. As we did in the discussion just after Lemma 2.2.2, fix a square root $\sqrt{\delta_j}$ of δ_j for $j \in \{1, \dots, 6\}$ (corresponding to ϵ_j in Example 2.2.10). Let us now determine the action of the absolute Galois group of \mathbb{Q} on the lines. By Lemma 2.2.8, it factors through the extension m of the splitting field $l = \mathbb{Q}(r_1, r_2, r_3)$ of f obtained by adjoining all elements of the form $\sqrt{\delta_i} \sqrt{\delta_j}$. Note that $\delta_1 \delta_2 = v_{11} v_{12} = N_{(\mathbb{Q}[X]/f_1)/\mathbb{Q}}(v_1)$ is a square by hypothesis. Similarly, letting Δ_1 denotes the discriminant of f_1 , we find that $\Delta_1 \delta_3 \delta_4$ and $\Delta_1 \delta_5 \delta_6$ are squares, and thus that $\delta_3 \delta_4$ and $\delta_5 \delta_6$ are squares in $\mathbb{Q}(\sqrt{\Delta_1}) = \mathbb{Q}(r_1)$. It follows that up to square factors in $\mathbb{Q}(r_1)$ every element of the form $\sqrt{\delta_i} \sqrt{\delta_j}$ is equivalent to $\delta_1 \delta_3$, $\delta_1 \delta_5$, or $\delta_3 \delta_5$. We conclude that $m = l(\sqrt{\delta_1} \sqrt{\delta_3}, \sqrt{\delta_1} \sqrt{\delta_5})$. As the v_i are otherwise generic, we find that the field m of definition of the lines has degree 4 over l and therefore degree 32 over \mathbb{Q} .

We now describe the Galois group of m over \mathbb{Q} in terms of the s, t described in the discussion following Proposition 2.2.11. The v_i are generic aside from their given properties, so the field $m' = l(\sqrt{\delta_1}, \dots, \sqrt{\delta_6}) = m(\sqrt{\delta_1})$ has degree 2 over m (cf. discussion following Lemma 2.2.2 and Example 2.2.10). Recall that for a permutation $p \in S_6$, the automorphism t_p of m is induced from m' by sending δ_j and $\sqrt{\delta_j}$ to $\delta_{p(j)}$ and $\sqrt{\delta_{p(j)}}$ respectively. For a subset $I \subseteq \{1, 2, \dots, 6\}$, the automorphism s_I of m is induced from m' by fixing all δ_j and sending $\sqrt{\delta_j}$ to $\pm \sqrt{\delta_j}$ where the sign is negative if and only if $j \in I$. We will also refer to the 32 lines on V using the notation L_I introduced before Lemma 2.2.3.

The automorphism σ_1 lifts to an automorphism of m' that fixes r_2 and r_3 , and therefore all δ_j for $3 \leq j \leq 6$. Because σ_1 sends $\sqrt{\Delta_1}$ to $-\sqrt{\Delta_1}$, and $\delta_3 \delta_4$ and $\delta_5 \delta_6$ are squares up to a factor Δ_1 , this lift changes the signs of the square roots of one of δ_3 and δ_4 and of one of δ_5 and δ_6 . The induced automorphism of m is then $t_{(12)} s_{i,j}$ for some $i \in \{3, 4\}$ and $j \in \{5, 6\}$. The automorphisms σ_2 and σ_3 lift to $t_{(34)}$ and $t_{(56)}$ respectively. Together with $s_{\{1,2\}}$ and $s_{\{3,4\}}$ these elements generate a subgroup of $\text{Gal}(m/\mathbb{Q})$ of order 32, so they generate the full Galois group. The orbits of this group on the lines are of order 8 and each orbit contains two nonintersecting lines from each of the four fibers of one fibration. In particular, all the four I_4 fibers are conjugate, so they are indeed defined over a field of degree 4.

By Remark 2.2.6 the fibers of the elliptic fibrations are orbits of Λ under the group generated by s_1 and s_2 in $\text{Aut } \Lambda$ (only their product $s_1 s_2$ is in the subgroup of $\text{Aut } \Lambda$ induced by Galois). Consider first the fibration associated to the exhibit \mathcal{S} that contains a 4-gon S containing L_0 . Then that 4-gon is $S = \{L_0, L_1, L_2, L_{12}\}$. One easily checks that the subgroup $\text{Gal}(m/k(S))$ is generated by $t_{(34)}$, $t_{(56)}$, and $s_{\{1,2\}}$. This group fixes $\mathbb{Q}(r_1)$, so we have $\mathbb{Q}(r_1) \subset k(S)$, and in fact the group $\text{Gal}(m/\mathbb{Q}(r_1))$ is generated by $\text{Gal}(m/k(S))$ and $s_{\{3,4\}}$. Under $\text{Gal}(m/k(S))$ the 4-gon S breaks up into the orbits $\{L_0, L_{12}\}$ and $\{L_1, L_2\}$, each consisting of two disjoint lines.

Let L be any line in S . The subgroup $\text{Gal}(m/k(L))$ is generated by $t_{(34)}$ and $t_{(56)}$, which is normal in $\text{Gal}(m/\mathbb{Q}(r_1))$. Therefore, $k(L)$ is Galois over $\mathbb{Q}(r_1)$ and the corresponding Galois group is $(\mathbb{Z}/2\mathbb{Z})^2$. Since $k(S)$ is one of the quadratic subfields, it follows from elementary Galois theory that $k(L)$ can be obtained from $k(S)$ by adjoining the square root of an element $c \in \mathbb{Q}(r_1)$. As $k(S)$ has degree 4 over \mathbb{Q} and $\mathbb{Q}(r_1)$ is a quadratic subextension, the norm of c from $k(S)$ to \mathbb{Q} is indeed a square. The arguments for the opposite fibration are completely similar.

The final statement of the proposition, that the elements of the vertical Brauer group obtained in this way give the same element of $H^1(\mathbb{Q}, \text{Pic } \bar{V})$, is proved by a calculation using MAGMA. The point is to verify that the images of the nontrivial elements of $H^1(\mathbb{Q}, \text{Pic}_\phi V)$ and $H^1(\mathbb{Q}, \text{Pic}_{\phi'} V)$ constructed in Proposition 3.1.10 in $H^1(\mathbb{Q}, \text{Pic } \bar{V})$ are equal, where ϕ and ϕ' are the two fibrations associated to the factorization $f = (f_1)(f_2 f_3)$ as in Remark 2.2.6. See [21] for details. \square

Remark 3.1.15 In special cases it is possible for the Picard group of V to have higher rank than in the generic case (in fact this happens in the example that we present immediately below). Thus we may have constructed elements, not of $H^1(\mathbb{Q}, \text{Pic } \bar{V})$, but only of $H^1(\mathbb{Q}, P)$, where P , the subgroup of $\text{Pic } \bar{V}$ generated by the classes of the lines, is a proper subgroup of $\text{Pic } \bar{V}$. The inclusion $P \rightarrow \text{Pic } \bar{V}$ gives a map from $H^1(\mathbb{Q}, P)$ to $H^1(\mathbb{Q}, \text{Pic } \bar{V})$, which allows us to consider the elements we have constructed as elements of the Brauer group. It is possible that our elements could be in the kernel of this map in some situations. However,

they are well-defined Brauer classes, and so they may be used to attempt to prove that V has no rational points. If their local invariants do not add to 0, it indicates that they are not in the kernel.

Remark 3.1.16 It is not essential for the method that the element of $H^1(\mathbb{Q}, \text{Pic } \bar{V})$ be obtainable from two different fibrations. However, as was first pointed out by Swinnerton-Dyer, this means that the local invariants are constant on the fibers of two different fibrations and is therefore much more likely to be constant than would otherwise be the case. This greatly facilitated finding the example below.

3.2 An explicit example

Now let us present our example, which was found by searching over various choices of f_1, f_2, f_3 with small splitting fields $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{5})$ such that the discriminant of $f_1 f_2 f_3$ is small and δ such that the field of definition of the lines would not introduce new bad primes. For the rest of this paper, let $f = (x^2 + 1)(x^2 - 2x - 1)(x^2 + x - 1) = f_1(x)f_2(x)f_3(x)$, let $A_f = \mathbb{Q}[X]/f(X)$, let E be the algebra $\mathbb{Q}(i) \oplus \mathbb{Q}(\sqrt{2}) \oplus \mathbb{Q}(\sqrt{5})$, fix an isomorphism $\iota : A_f \rightarrow E$ as in Definition 3.1.13, and let

$$\delta = (-2X^5 + 3X^4 + 5X^3 - 8X^2 + 7X + 7)/6 \quad (5)$$

be the element of A_f , so that $\iota(\delta) = (3, -(1 + \sqrt{2}), (1 + \sqrt{5})/2)$. Then f, δ satisfy the conditions of Theorem 3.1.14. For nonzero rational t let C_t be the curve $y^2 = tf(x)$. Let V be the K3 surface $V_{f, \delta}$. Our goal is to prove the main theorem, Theorem 1.0.1, restated and slightly reworded here for ease of reading:

Theorem 3.2.1 *Let S be the union of $\{5\}$ with the set of primes that split completely in the field of definition of the lines of V , which is*

$$F = \mathbb{Q} \left(\sqrt{-1}, \sqrt{2}, \sqrt{5}, \sqrt{-3(1 + \sqrt{2})}, \sqrt{6(1 + \sqrt{5})} \right).$$

Then for all n which are products of elements of S , the 2-part of the Tate-Shafarevich group of the Jacobian of the curve C_{-6n} is nontrivial.

To do so, we will follow the strategy outlined in the introduction: first we will show that δ gives an element of the fake Selmer group of the curve in question by showing that the corresponding principal homogeneous space of the Jacobian of C_{-6n} has points everywhere locally. Then we will use the element of the Brauer group described above to prove that $V_{f, \delta}$ has no rational points and conclude that the principal homogeneous space has no rational points either. We begin by summarizing some results from [18] on the fake Selmer group of a hyperelliptic curve of genus 2.

Definition 3.2.2 *Let g be a squarefree polynomial of degree 6 over \mathbb{Q} and C the curve $y^2 = g(x)$. For any field K of characteristic 0, let $H_K = \ker(N : (A_g \otimes K)^*/(A_g \otimes K)^{*2} K^* \rightarrow K^*/K^{*2})$ with $A_g = \mathbb{Q}[X]/g(X)$. (Note that the norm is well-defined, because $\deg g$ is even and so $N(K^*) \subset K^{*2}$.) Write H instead of $H_{\mathbb{Q}}$. As in [18], Prop. 5.5, let the fake Selmer group $\text{Sel}_{\text{fake}}^{(2)}(\mathbb{Q}, \text{Jac } C)$ of C be the subgroup of H consisting of elements that are everywhere locally in the image of the 2-descent map on the Jacobian of C . Define Δ_K , the descent map over K , to be the function from the set of K -rational points of C which are neither Weierstrass points nor points at infinity to H_K such that $\Delta_K(x_0, y_0) = 1 \otimes x_0 - X \otimes 1$.*

Proposition 3.2.3 *The function Δ_K may be extended multiplicatively to a function from $J(K)$ to H_K .*

Proof. This is essentially [15], Lemma 2.1, as modified by the discussion in section 2.5; see also [18], sect. 6 for explicit formulas for Weierstrass points. \square

Proposition 3.2.4 *Let S be the set of primes introduced in Theorem 3.2.1. Then for all n that are products of elements of S , the fake Selmer group of the Jacobian of C_{-6n} contains δ . Equivalently, the principal homogeneous space of $\text{Jac}(C_{-6n})$ corresponding to δ is everywhere locally solvable.*

Proof. We need only show that δ is in the image of the local Selmer maps for primes of bad reduction and ∞ . The primes of bad reduction are 2, 3, 5, and primes dividing n . At a prime p dividing n , we have that δ corresponds under ι to an element of the form $(3, 3a^2, 3b^2)$ in $E \otimes \mathbb{Q}_p$. Therefore, δ is contained in $(A_f \otimes \mathbb{Q}_p)^{*2} \mathbb{Q}_p^*$, so it is the identity element in $H_{\mathbb{Q}_p}$ and is in the image of every homomorphism. Thus δ is in the image of the local 2-descent map. Note also that every product of elements of S is positive, is equivalent to 1 or 5 in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ for $p = 2, 5$, and is a unit locally at 3. It follows that we need only check the assertion for $n = 1, p = 2, 3, 5, \infty$, and $n = 5, p = 2, 3, 5$. This can be done by using MAGMA's `TwoSelmerGroup` command to compute the fake Selmer groups of C_{-6} and $C_{-6.5}$ and verifying that δ is an element of both. The last statement follows by applying the fact that the principal homogeneous space over a field K corresponding to δ has points if and only if δ is in the image of Δ_K to all completions of \mathbb{Q} . \square

Proposition 3.2.5 *Assume Stoll's condition (\dagger) (this is automatic for curves of even genus). If the image of $\text{Jac}(C_t)/2 \text{Jac}(C_t)$ under the 2-descent map $\Delta_{\mathbb{Q}}$ is properly contained in the fake Selmer group, then $\text{Jac}(C_t)$ has nontrivial Tate-Shafarevich group.*

Proof. Let $c = \dim \text{Sel}^{(2)} \text{Jac}(C_t) - \dim \text{Sel}_{\text{fake}}^{(2)} \text{Jac}(C_t)$ and let d be the dimension of the ‘‘Cassels kernel’’ of $\text{Jac}(C_t)$, namely, the kernel of the descent map modulo $2 \text{Jac}(C_t)$. Since we are assuming condition (\dagger) , we have $c = 0$ if and only if condition (\ddagger) , and condition (\ddagger) implies that $d = 0$. Both c and d are at most 1, so $c \geq d$. Under the assumptions of the proposition, it follows that

$$\begin{aligned} \dim \text{Sel}^{(2)} \text{Jac}(C_t) &= \dim \text{Sel}_{\text{fake}}^{(2)} \text{Jac}(C_t) + c \\ &> \dim \text{im } \text{Jac}(C_t) + c \\ &\geq \dim \text{im } \text{Jac}(C_t) + d \\ &= \dim \text{Jac}(C_t)/2 \text{Jac}(C_t), \end{aligned}$$

from which the conclusion is immediate. \square

Now we indicate the relation between the descent map and the K3 surface $V_{f,\delta}$ that we have defined.

Proposition 3.2.6 *With f and δ as above, let V be the K3 surface constructed from f, δ . Suppose that V has no rational points. Then δ is not in the image of the 2-descent map for the Jacobian of the curve $y^2 = f(x)$.*

Proof. Suppose, to the contrary, that δ were in the image; that is, that $\Delta_{\mathbb{Q}}(D) = \delta$ for some divisor D of degree 0. By Riemann-Roch, this divisor may be taken to be of the form $(x_1, y_1) + (x_2, y_2) - H$, where H is the hyperelliptic divisor. Since $\Delta_{\mathbb{Q}}(H) = 1$, this means that $\Delta_{\mathbb{Q}}(D) = \Delta_{\mathbb{Q}}((x_1, y_1) + (x_2, y_2)) = (x_1 - X)(x_2 - X)$ in $A_f^*/(A_f^*)^2 \mathbb{Q}^*$, where we have identified $A_f \otimes_{\mathbb{Q}} \mathbb{Q}$ with A_f . In other words, for some $r \in \mathbb{Q}$ and $q \in A_f$ we have $\delta q^2 = r x_1 x_2 - r(x_1 + x_2)X + rX^2$. In particular, the point of \mathbb{P}^5 whose coordinates are the coefficients of q lies on V . \square

Remark 3.2.7 Propositions 3.2.5 and 3.2.6 together imply that if δ is an element of the fake Selmer group $\text{Sel}_{\text{fake}}^{(2)}(\mathbb{Q}, \text{Jac } C_t)$ and the corresponding $V_{f,\delta}$ has no rational points, then $\text{Jac}(C_t)$ has nontrivial Tate-Shafarevich group. This also follows from the fact that $V_{f,\delta} = V_{tf,\delta}$ is a quotient of the homogeneous space of $\text{Jac } C_t$ corresponding to δ . Indeed, this implies that if $V_{f,\delta}$ has no rational points, then neither does the homogeneous space, which implies its image in the Tate-Shafarevich group is nontrivial.

It is also worth mentioning that the existence of the nontrivial element of III that we will exhibit is not a consequence of the results of [14] on odd curves, which we now describe briefly.

Definition 3.2.8 ([14]) *Let C be a curve over \mathbb{Q} of genus g . We say that C is deficient at p , where p is a prime or ∞ , if C has no rational divisor of degree $g - 1$ over \mathbb{Q}_p . We say that C is even or odd depending on the parity of the number of places at which C is deficient.*

Denote the 2-primary part of $\text{III}(\text{Jac}(C))$ by $\text{III}(\text{Jac}(C))[2^\infty]$. Then, if $\text{III}(\text{Jac}(C))[2^\infty]$ is finite, its order is a square if and only if C is even ([14], Theorem 11). It follows that if C is odd that $\text{III}(\text{Jac}(C))[2^\infty]$ is nontrivial. The following proposition proves that the elements of III that we find are not merely artifacts of the oddness of our curves.

Proposition 3.2.9 *If n is a product of primes in S , then C_{-6n} is even.*

Proof. A curve is never deficient at a prime p of good reduction, for there are always points over all sufficiently large finite fields of characteristic p and therefore over unramified extensions of \mathbb{Q}_p of all sufficiently large degrees. The primes of bad reduction are 2, 3, 5, and those dividing n . The point $(i, 0)$ on C_{-6n} is defined over \mathbb{Q}_p for all p congruent to 1 mod 4, which includes 5 and all primes dividing n . It is also clear that there are real points on C_{-6n} . As a result, the only primes that need to be considered are 2 and 3. One checks (for example, using the `IsDeficient` command in MAGMA) that C_{-6n} is deficient at those primes. It follows that C_{-6n} is even. \square

We now start to show that V has no rational points, from which it follows that δ is not in the image of the global 2-descent map. First we will limit the set of primes to be considered in the calculation of the Brauer-Manin obstruction, then we will explain how to calculate the invariants there, and after that we will actually compute the invariants.

Lemma 3.2.10 *Let W be a variety over \mathbb{Q} with good reduction at p and let $s \in \text{Br } W$. Then the local invariant of s at p is constant.*

Proof. This is a weaker version of Theorem 1 of [5]. \square

Lemma 3.2.11 *Let W be an elliptic surface over \mathbb{Q} with an Azumaya algebra s given by $\text{cores}(c, t - \alpha)$ as in Proposition 3.1.10. Let p be a prime of good reduction for W such that the fiber at infinity of W has smooth \mathbb{Q}_p -rational points (in particular, this is true if the fiber at infinity has good reduction mod p). Then the local invariant of s at p is equal to 0.*

Proof. By Lemma 3.2.10, the local invariant is constant, so it suffices to evaluate it at one point. Since the fiber at infinity has smooth \mathbb{Q}_p -rational points, so do all sufficiently near fibers. In particular, for all sufficiently large integers k the fiber at p^{-2k} has rational points, and the local invariant is therefore

$$\text{cores}(p^{-2k} - \alpha, c) = \sum_{\mathfrak{p}|p} (p^{-2k} - \alpha, c)_{\mathfrak{p}}.$$

But $p^{-2k} - \alpha$ is a square in all completions at primes above p for all sufficiently large k , and hence the local invariant is 0 for sufficiently large k . \square

Lemma 3.2.12 *Let W be an elliptic surface over \mathbb{Q} with an Azumaya algebra $\text{cores}(c, t - \alpha)$, where c has square norm. Suppose that the valuation of $\alpha/4p^n$ is positive at all primes above p at which c is not a square. Then the invariant at p is 0 on all fibers of coordinate t where $v(t) \leq n$.*

Proof. We notice that $t/(t - \alpha)$ is a square for all t with $v(t) \leq n$, and therefore that the invariants of (c, t) and $(c, t - \alpha)$ are equal at all primes above p where c is not a square. They are also equal at primes above \mathfrak{p} at which c is a square, being both equal to 0 there, so they are equal at all primes above p . Thus the invariant at p of $\text{cores}(c, t - \alpha)$ is equal to that of $\text{cores}(c, t)$ (see Proposition 3.1.12). But this is equal to the invariant of $(N(c), t)$, which is 0 because $N(c)$ is a square. \square

Lemma 3.2.13 *Let $t_0 \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$ be such that $p^n/4(t_0 - \alpha)$ has positive valuation in $\mathbb{Q}(\alpha)_{\mathfrak{p}}$ for all primes \mathfrak{p} above p where c is not a square locally. Then the local invariant of the Azumaya algebra $\text{cores}(c, t - \alpha)$ is the same for all values of t in the disc $t_0 + p^n\mathbb{Z}_p$.*

Proof. It is sufficient to show that $(t - \alpha)/(t_0 - \alpha)$ is a square for all $t \in t_0 + p^n\mathbb{Z}_p$ at all primes \mathfrak{p} above p where c is not a square. But this is equal to $1 + kp^n/(t_0 - \alpha)$ for some $k \in \mathbb{Z}_p$, which by assumption is congruent to 1 mod $4\mathfrak{p}$. It is therefore a square by Hensel's lemma. \square

Lemma 3.2.14 *It can be effectively determined whether there are \mathbb{Q}_p -rational points of V mapping under a given fibration to a given disc D in $\mathbb{P}^1(\mathbb{Q}_p)$.*

Proof. By changing coordinates, we may assume that the disc is $\{(\mathbb{Z}_p : 1)\}$. Consider the graph of the fibration as a subscheme of $\mathbb{P}^5 \times \mathbb{P}^1$. It is sufficient to determine whether there is a standard affine patch \mathbb{A}^5 of \mathbb{P}^5 such that the intersection of the patch $\mathbb{A}^5 \times D$ of $\mathbb{P}^5 \times \mathbb{P}^1$ with the graph of the fibration has \mathbb{Z}_p -points. Since the graph is smooth, this can be determined using Hensel's lemma. \square

Theorem 3.2.15 *Let V be a smooth variety with an elliptic fibration ϕ over \mathbb{P}^1 satisfying the hypotheses of Proposition 3.1.10 and let $\text{cores}(c, t - \alpha) \in \text{Br } \phi$ be the Azumaya algebra constructed there. Let p be a prime. Then the set of values of the local invariant of $\text{cores}(c, t - \alpha)$ on $V(\mathbb{Q}_p)$ can be effectively determined.*

Proof. Using Hensel's lemma or Lemma 3.2.14 we can check whether V has any \mathbb{Q}_p -points. If not, then we are done, so we may assume that V has \mathbb{Q}_p -points. If V has good reduction at p , then by Lemma 3.2.10 the local invariant $\text{cores}(c, t - \alpha)$ is constant, so it suffices to evaluate it at one point of V . Since V is nonsingular, its \mathbb{Q}_p -points are dense, so we can find a point for which $t - \alpha$ is bounded away from 0 and ∞ . It is then easy to compute the local invariant there.

We will describe the algorithm for calculating the values of the local invariant of $\text{cores}(c, t - \alpha)$ at a prime p of bad reduction for V and then prove that it terminates. The point is that this local invariant turns out to be locally constant. In fact, we will show how to find an explicit finite covering of $\mathbb{P}^1(\mathbb{Q}_p)$ by discs in the p -adic topology, such that for each disc the invariant is constant on the set of \mathbb{Q}_p -points on V mapping to that disc under the elliptic fibration.

First we show that such a disc exists around each point in $\mathbb{P}^1(\mathbb{Q}_p)$, starting with the point at infinity. After a change of variables we may assume that the fiber at $t = \infty$ is smooth over \mathbb{Q}_p . If the fiber at ∞ does have points over \mathbb{Q}_p , then by Lemma 3.2.12 we can find an n such that the local invariant is 0 on all points on fibers above t with $v(t) < n$. In this case the disc $v(t) < n$ has the desired property. If the fiber at $t = \infty$ does not have any \mathbb{Q}_p -points, then there is a p -adic neighborhood of $\infty \in \mathbb{P}^1(\mathbb{Q}_p)$ above which there are no \mathbb{Q}_p -points either, so the invariant is clearly constant above any disc contained in this neighborhood.

Now observe that, by Lemma 3.2.13, every finite t_0 has a suitable neighborhood except for those that are roots of the minimal polynomial of α , so we are reduced to considering the finite set of these t_0 . Here the argument will be more subtle. Fix such t_0 and let \mathfrak{p} be the corresponding place of $\mathbb{Q}(\alpha)$, so that the completion map $\rho: \mathbb{Q}(\alpha) \hookrightarrow \mathbb{Q}(\alpha)_{\mathfrak{p}}$ sends α to t_0 . Here we used the obvious embedding $\mathbb{Q}_p \hookrightarrow \mathbb{Q}(\alpha)_{\mathfrak{p}}$, which is an isomorphism as α is contained in \mathbb{Q}_p .

First consider the case that the fiber above $t = t_0 = \rho(\alpha)$ does have a point P over $\mathbb{Q}_p \cong \mathbb{Q}(\alpha)_{\mathfrak{p}}$. Then P must be a smooth point of the $\mathbb{Q}(\alpha)_{\mathfrak{p}}$ -component it lies on, because by hypothesis each $\mathbb{Q}(\alpha)$ -component is smooth. Therefore the geometric component on which P lies is defined over $\mathbb{Q}(\alpha)_{\mathfrak{p}} \cong \mathbb{Q}_p$, so by hypothesis all geometric components of the fiber at $t = t_0 = \rho(\alpha)$ are defined over \mathbb{Q}_p , which means that $\rho(c)$ is a square. For all other places \mathfrak{q} above p the embedding $\mathbb{Q}_p \hookrightarrow \mathbb{Q}(\alpha)_{\mathfrak{q}}$ does not send t_0 to α , so we can find an integer n such that under each such embedding the element $p^n/4(t_0 - \alpha)$ has positive valuation in $\mathbb{Q}(\alpha)_{\mathfrak{q}}$. By Lemma 3.2.13 the invariant is constant above the disc $t_0 + p^n\mathbb{Z}_p$. In the implementation of this algorithm it will be useful to remember that c is a square in $\mathbb{Q}(\alpha)_{\mathfrak{p}}$, as this implies that the local invariant corresponding to the place \mathfrak{p} is 0 globally. In the case that the fiber above $t = t_0$ does not have any \mathbb{Q}_p -points, there is a p -adic neighborhood of $t_0 \in \mathbb{P}^1(\mathbb{Q}_p)$ above which there are no \mathbb{Q}_p -points either, so the invariant is constant above any disc contained in this neighborhood.

The algorithm is as follows. First apply a change of coordinates to \mathbb{P}^1 if necessary, so that the fiber at infinity is smooth. Then find a neighborhood of infinity above which the local invariant is constant. This reduces to considering t in some set of the form $p^n\mathbb{Z}_p$. For each t_0 that maps to α in $\mathbb{Q}(\alpha)_{\mathfrak{p}}$ for some

place \mathfrak{p} above p , find an appropriate disc around t_0 . In doing so we may find that the value of the local invariant corresponding to some \mathfrak{p} is 0 for all \mathbb{Q}_p -points of V . Such \mathfrak{p} can be ignored in the remainder of the computation. If there are points above any of the discs found thus far, compute the corresponding local invariants.

We now divide the remaining region of $\mathbb{P}^1(\mathbb{Q}_p)$ into discs and place them in a queue, recording which local invariants we already know to occur. For each disc, we use Lemma 3.2.13 to try to discover that the local invariant is constant there. If it is, and if the local invariant is already known to occur, the disc may be ignored, as the conclusions do not depend on whether there are rational points there. If it is, and if the local invariant is *not* already known to occur, we use Lemma 3.2.14 to test whether there are rational points in that disc. If there are rational points on the disc, we record that the invariant on the disc occurs. The only possible values of the invariant of an element of $\text{Br } V / \text{Br } \mathbb{Q}$ of order 2 are $0, \frac{1}{2} \in \mathbb{Q}/\mathbb{Z}$; if both of these are now known to occur, we are done. On the other hand, if the local invariant is not constant on the disc, we divide it into p smaller discs and add them to the end of the queue. In other words, we perform a breadth-first search. The reason for using breadth-first rather than depth-first search is that local invariants are more likely to be different on relatively distant points of a p -adic disc, so breadth-first search will tend to find different invariants more quickly. When the queue is empty we are done and have recorded all values of the local invariant.

Now we show that this algorithm terminates. It could fail to do so only if there is an infinite descending sequence of discs above which there are rational points but in which the local invariant is not constant. Let t_0 be the unique point in the intersection of the discs. Then we have shown before that there is a disc around t_0 on which the local invariant of $\text{cores}(c, t - \alpha)$ is constant, which is a contradiction, so the algorithm does terminate. \square

Remark 3.2.16 This theorem is somewhat special to our situation. If the Azumaya algebra were constructed using fibers of type I_2 , for example, this proof would not apply, and indeed in this case the local invariant associated to a place \mathfrak{p} above p need not be locally constant on \mathbb{P}^1 around a t_0 that maps to α in $\mathbb{Q}(\alpha)_{\mathfrak{p}}$.

Let us now show how to apply this algorithm in our example.

Proposition 3.2.17 *The Brauer-Manin obstruction blocks the existence of rational points on the K3 surface V corresponding to (f, δ) .*

Proof. The surface V is defined by the equations $q_1 = q_2 = q_3 = 0$, where

$$\begin{aligned} q_1 &= x_1^2 + 2x_1x_3 + 8x_1x_4 + 10x_1x_5 + 24x_1x_6 + x_2^2 + 8x_2x_3 + 10x_2x_4 + 24x_2x_5 + 58x_2x_6 + 5x_3^2 + 24x_3x_4 \\ &\quad + 58x_3x_5 + 152x_3x_6 + 29x_4^2 + 152x_4x_5 + 346x_4x_6 + 173x_5^2 + 856x_5x_6 + 1017x_6^2, \\ q_2 &= x_1x_2 + 2x_1x_3 + 3x_1x_4 + 6x_1x_5 + 17x_1x_6 + x_2^2 + 3x_2x_3 + 6x_2x_4 + 17x_2x_5 + 40x_2x_6 + 3x_3^2 + 17x_3x_4 \\ &\quad + 40x_3x_5 + 97x_3x_6 + 20x_4^2 + 97x_4x_5 + 230x_4x_6 + 115x_5^2 + 563x_5x_6 + 675x_6^2, \\ q_3 &= 6x_1x_3 + 8x_1x_4 + 12x_1x_5 + 30x_1x_6 + 3x_2^2 + 8x_2x_3 + 12x_2x_4 + 30x_2x_5 + 84x_2x_6 + 6x_3^2 + 30x_3x_4 + 84x_3x_5 \\ &\quad + 192x_3x_6 + 42x_4^2 + 192x_4x_5 + 466x_4x_6 + 233x_5^2 + 1112x_5x_6 + 1360x_6^2. \end{aligned}$$

The primes of bad reduction of V are those dividing the discriminant of f , namely 2, 3, 5, and those involved in δ , which are again 2, 3, 5. Each of the fibrations is defined by two alternative pairs of linear forms (see Lemma 2.3.5 and following remarks). We let

$$\begin{aligned} l_1 &= x_1 + 13x_3 + 17x_4 + 68x_5 + 123x_6, \\ l_2 &= x_2 - 16x_3 - 19x_4 - 84x_5 - 145x_6, \\ l_3 &= 2x_2 - 8x_3 - 8x_4 - 42x_5 - 68x_6, \\ l_4 &= -x_1 - 4x_2 + 9x_3 + 5x_4 + 46x_5 + 61x_6, \end{aligned}$$

and then one of the fibrations, which we will denote by F_1 , is given by $(l_1 : l_2)$ or $(l_3 : l_4)$, while the other, which will be written F_2 , is given by $(l_1 : l_3)$ or $(l_2 : l_4)$. To verify that the two sets of defining equations for each F_i give the same map, note that $l_1 l_4 - l_2 l_3 = -q_1 - 4q_2 + q_3$. We have already seen that F_1 satisfies the hypotheses of Proposition 3.1.10; now we calculate the local invariant of the associated Azumaya algebra by means of the algorithm described in Theorem 3.2.15. We will show that this Azumaya algebra has local invariant $1/2$ at 2 and 0 at all other primes; the energetic reader may wish to verify that the Azumaya algebra corresponding to F_2 has local invariant $1/2$ at $2, 3$, and 5 , and local invariant 0 elsewhere.

The I_4 -fibers of F_1 lie over the point $(129r^3 + 187r^2 + 285r - 1469)/449$, where $r^4 - 12r + 13 = 0$. The fact that this extension is totally complex implies that the local invariant at ∞ is 0 , because that local invariant is the sum of local invariants of central simple algebras over \mathbb{C} . The components of these fibers are defined over the extension $\mathbb{Q}(r, \sqrt{c})$ where $c = -6r^3 - 9r^2 - 12r + 57$ (note that actually c has minimal polynomial $r^2 - 6r + 18$, so $c \in \mathbb{Q}(i)$, as expected from the proof of Theorem 3.1.14).

The fiber at ∞ is the vanishing locus of the polynomials

$$\begin{aligned} & x_1 + 55x_3 + 71x_4 + 290x_5 + 519x_6, \\ & x_2 - 16x_3 - 19x_4 - 84x_5 - 145x_6, \\ & x_3^2 + 414x_3x_4 - 4538x_3x_5 - 5876x_3x_6 + 448x_4^2 - 3796x_4x_5 - 4200x_4x_6 - 23754x_5^2 - 73732x_5x_6 - 56083x_6^2, \\ & 7596x_3x_4 - 83956x_3x_5 - 108804x_3x_6 + 8241x_4^2 - 70306x_4x_5 - 77950x_4x_6 - 438959x_5^2 - 1362754x_5x_6 - 1036791x_6^2, \end{aligned}$$

and it has good reduction outside $2, 3, 5, 397, 449$. This can be checked either by a Groebner-basis computation or by embedding the fiber in \mathbb{P}^3 as the curve defined by two quadrics Q_1, Q_2 and observing that the curve is nonsingular away from primes dividing the discriminant of $\det(tM_1 + M_2)$, where M_1 and M_2 are the symmetric matrices corresponding to Q_1, Q_2 . By Lemma 3.2.11, the local invariant at every other prime is 0 . We examine these primes in turn.

First we consider $p = 2$. We find that there are no rational points in the fibers over t with $v_2(t) \leq 1$. In fact, none of the affine patches of the graph of the fibration (see Lemma 3.2.14) has points mod 2^3 for such t . On the other hand, the point $[1 : 0 : 5 : 3 : 6 : 1]$ modulo 8 can be lifted to a 2 -adic point on the fiber at 0 . Let us show that the local invariant is $1/2$ above all t with $v_2(t) \geq 2$. Indeed, by Lemma 3.2.13 it suffices to consider $t = 0, 4$. There is one prime \mathfrak{p} of $\mathbb{Q}(r)$ above 2 , and it is totally ramified. Therefore it suffices to show that the conics $x^2 - (t - \alpha)y^2 - cz^2$ are not solvable at \mathfrak{p} for $t = 0, 4$. In both cases this can be checked modulo \mathfrak{p}^5 .

Next we consider $p = 3$. This time we find that there are no rational points in fibers above t with $v_3(t) \leq -1$, and that this can be checked modulo 3^2 . However, the point $[8 : 0 : 7 : 4 : 2 : 1]$ modulo 9 can be lifted to a 3 -adic point on the fiber at 4 . Let us show that the local invariant is 0 above all t with $v_3(t) \geq 0$. Again, by Lemma 3.2.13 it suffices to consider $t = 0, 1, 2$. There are two primes of $\mathbb{Q}(r)$ lying above 3 , both unramified of degree 2 , and c has valuation 1 at both. On the other hand, α has valuation 0 at both primes and α is not congruent to any integer modulo either prime. Furthermore, $2 - \alpha$ is a square at both, while $-\alpha$ and $1 - \alpha$ are squares at neither. In particular, it follows from Lemma 3.1.9 that the local invariant at t is 0 above all $t \in \mathbb{Z}_3$.

For $p = 5$, the computations are simpler, because c is a square at all primes of $\mathbb{Q}(r)$ lying above 5 . Indeed, there is one ramified prime at which the completion is isomorphic to $\mathbb{Q}_5(\sqrt{5})$ and c is congruent to $4 \bmod \sqrt{5}$, and one unramified prime of degree 2 at which c is congruent to $2 \bmod 5$, which is a square in \mathbb{F}_{25} . Thus the local invariant is 0 above all $t \in \mathbb{P}^1(\mathbb{Q}_5)$.

Finally, we need to consider the primes where V has good reduction but the fiber at infinity has bad reduction, namely 397 and 449 . Note that c is a unit at every place above 397 . Also, for every point P whose image t_P in \mathbb{P}^1 is not congruent to $\alpha \bmod \mathfrak{p}$ above 397 , the difference $t_P - \alpha$ is a unit at all \mathfrak{p} above 397 . Proposition 3.1.9 then shows that the local invariant of $(c, t_P - \alpha)$ is 0 at all such \mathfrak{p} , so that the local invariant of $\text{cores}(c, t_P - \alpha)$ is 0 by Proposition 3.1.12. every \mathbb{Q}_{397} -point on V whose reduction mod p does not lie on an I_4 -fiber will have local invariant 0 . Over \mathbb{F}_{397} , the I_4 -fibers lie above $(47 : 1)$, $(144 : 1)$, $(224 : 1)$, $(379 : 1)$ (the first coordinates are the roots of the minimal polynomial of α in \mathbb{F}_{397}). Since V has good reduction at 397 , every \mathbb{F}_{397} -point on V lifts to a \mathbb{Q}_{397} -point, so it suffices to verify that the \mathbb{F}_{397} -point

$(246 : 16 : 98 : 0 : 1 : 0)$ maps to $(0 : 1)$ by F_1 . But by Proposition 3.2.10, it follows that the local invariant at 397 is identically 0.

To prove that the local invariant at 449 is 0, it is enough to check that c is a square at all places of $\mathbb{Q}(r)$ above 449: indeed, it is congruent to 204 or 251 at all of these places. Alternatively, it can be verified that the fiber at infinity contains a \mathbb{Q}_{449} -point lying above $(246 : 105 : 375 : 347 : 1 : 0)$. This completes the proof. \square

Theorem 3.2.1 now follows by combining Propositions 3.2.4, 3.2.5, 3.2.6, and 3.2.17.

3.3 The Richelot isogeny

Following a suggestion of Nils Bruin and Victor Flynn, we now study the interaction of the element of III constructed in Theorem 3.2.1 with the Richelot isogeny on the Jacobian. A Richelot isogeny (cf. [7], chapter 9) is an isogeny of the Jacobian of a curve of genus 2 to that of another curve whose kernel is a maximal isotropic subgroup of the 2-torsion. Given a curve of genus 2 with Weierstrass points W_1, \dots, W_6 , such subgroups consist of 0 and three divisors of the form $W_i - W_j$ such that no W_i appears in more than one of them; since $W_i - W_j = W_j - W_i$ in the Jacobian, they correspond to partitions of the Weierstrass points into two pairs. Letting the equation of the curve be $y^2 = f(x)$, where $\deg f = 6$, the Weierstrass points are $(\delta_i, 0)$ where δ_i is a root of f , so such partitions correspond to factorizations of f as products $f_1 f_2 f_3$ of three quadratic factors. The isogenous curve is then defined by the equation $y^2 = c g_1 g_2 g_3$, where $g_i = f_{i+1} f'_{i+2} - f'_{i+1} f_{i+2}$, indices are read mod 3, and c is the determinant of the matrix of coefficients of the f_i ([7], sect. 9.2). Observe that multiplying one of the f_i by a constant k multiplies c , g_{i+1} , and g_{i+2} by k . This is compatible with the evident fact that if C is isogenous to C' then the twist of C by k is isogenous to the twist of C' by k . In particular we find that the Jacobian of the curve

$$C_t : y^2 = t(x^2 + 1)(x^2 - 2x - 1)(x^2 + x - 1)$$

is isogenous to that of

$$C'_{-t} : y^2 = -t(x^2 + 1)(x^2 + 2x - 1)(x^2 - 4x - 1) = -t g_1(x) g_2(x) g_3(x) = -t g(x).$$

In addition we observe that there is only one rational Richelot isogeny on each of these curves, because the 2-torsion points that are not rational are defined over extensions of degree 4. A Galois-stable subgroup containing such a point contains four elements other than the identity, so it cannot have order 4. It follows that the only rational maximal isotropic subgroup is the one made up of the four rational points. From now on, we will denote the Richelot isogeny from $\text{Jac}(C_t)$ to $\text{Jac}(C'_{-t})$ by ϕ_t .

First we note that $\text{III}(\text{Jac}(C'_{-6n}))$ is also nontrivial for n in the set S described in Theorem 3.2.1.

Theorem 3.3.1 *Let S be the set of primes described in Theorem 3.2.1. Then for all n which are products of elements of S , the 2-part of the Tate-Shafarevich group of the Jacobian of the curve $y^2 = -6ng(x)$ is nontrivial.*

Proof. The proof of this theorem is very similar to that of Theorem 3.2.1, except that one uses $\delta' = (3, 1 + \sqrt{2}, (1 + \sqrt{5})/2)$. Note that the field of definition of the lines of $V_{g, \delta'}$ turns out to be the same as that of $V_{f, \delta}$, because -1 is a square in the splitting field of g . \square

It is natural to ask whether these systematically-occurring elements of III are in the kernel of the map induced on Tate-Shafarevich groups by ϕ_n . It is not clear whether a general result can be obtained here. We will prove only that they are not in the kernel for the smallest case $n = 1$. To do so, we will calculate the Selmer groups of these isogenies, as in [15], in the special case $n = 1$.

We now sketch the method of [15] for calculating Selmer groups. Let C be a curve and $\text{Jac } C$ its Jacobian. Let A be an abelian variety and $\phi : A \rightarrow J$ an isogeny from A to J . Let $\hat{\phi}$ be the dual isogeny from \hat{J} to \hat{A} . Then we find divisors D_1, \dots, D_r the union of whose Galois orbits spans $\ker \hat{\phi}$, and functions ψ_1, \dots, ψ_r such that the divisor of ψ_i is kD_i , where k is the exponent of $\ker \phi$ (here 2). The

functions ψ_i are defined over number fields $K(D_i)$; we use them to define an evaluation map from an open subset of $C(K)$ to $\oplus_i (K \otimes_{\mathbb{Q}} K(D_i))^*$ for every extension K of \mathbb{Q} , and hence a descent map $\delta_{\phi, C}$ from $J(\mathbb{Q})$ to $\oplus_i K(D_i)^*/K(D_i)^{*2}$, extending the evaluation map from points of C to divisors supported on an open subset of C by multiplicativity. It is proved in [15], Lemma 2.1, that this yields a well-defined map on the Jacobian. As in the usual descent procedure, the image is always contained in the subgroup of $\oplus_i K(D_i)^*/K(D_i)^{*2}$ unramified away from 2, ∞ , and the bad primes of J , which are a subset of the bad primes of C ([15], page 454). Provided that Schaefer's Assumptions I and II are satisfied, the Selmer group Sel_{ϕ} of ϕ is then isomorphic to the subgroup of $\oplus_i K(D_i)^*/K(D_i)^{*2}$ of elements unramified away from 2, ∞ , and bad primes of J which are in the images of the local descent maps at 2, ∞ , and the bad primes of J . Assumption I is satisfied because every rational divisor class on a curve of genus 2 is represented by a rational divisor, and Assumption II is satisfied because the natural map from $A[\phi]$ to $\mu_2(\mathbb{Q} \oplus \mathbb{Q})$ given by the Weil pairing is an isomorphism (this is because there is a Galois-invariant basis for $\ker \phi$, not merely a Galois-invariant spanning set).

Definition 3.3.2 *With notation as in the discussion above, the Tate-Shafarevich group III_{ϕ} is defined to be $\text{Sel}_{\phi}/\delta_{\phi, C}(J(\mathbb{Q}))$.*

Lemma 3.3.3 *The Selmer group Sel_{ϕ_n} of ϕ_n is a subgroup of $(\mathbb{Q} \oplus \mathbb{Q})^*/(\mathbb{Q} \oplus \mathbb{Q})^{*2}$, and the descent map $\delta_{\phi_n, C}$ takes a K -point (x, y) of C_n to $(f_1(x), f_2(x)) \in (K \oplus K)^*/(K \oplus K)^{*2}$. For C'_n the Selmer group is again a subgroup of $(\mathbb{Q} \oplus \mathbb{Q})^*/(\mathbb{Q} \oplus \mathbb{Q})^{*2}$, and the descent map corresponding to the isogeny dual to ϕ_n takes a K -point (x, y) of C'_n to $(g_1(x), g_2(x)) \in (K \oplus K)^*/(K \oplus K)^{*2}$.*

Proof. We will only prove this for C_n , the proof for C' being identical. Let D be a rational divisor class of order 2. Then D is represented by a divisor $(\alpha, 0) + (\alpha', 0) - D_{\infty}$, where α and α' are roots of one of the quadratic factors of f and D_{∞} is the divisor of poles of the function x on the curve. It follows that $2D$ is the divisor of the quadratic factor of f whose roots are α, α' . The kernel of ϕ_n is isomorphic to $(\mathbb{Z}/2)^2$ with trivial Galois action, so any two factors of f give functions whose divisors are doubles of the divisors that span the kernel. Since the factors are defined over \mathbb{Q} and we use two of them, the description of Schaefer's procedure above states that the descent map and its target are as claimed. \square

Proposition 3.3.4 *There is an exact sequence*

$$0 \rightarrow J(\mathbb{Q}_p)[\phi]/\phi'(J'(\mathbb{Q}_p)[2]) \rightarrow J(\mathbb{Q}_p)/\phi'(J'(\mathbb{Q}_p)) \rightarrow J'(\mathbb{Q}_p)/2J'(\mathbb{Q}_p) \rightarrow J'(\mathbb{Q}_p)/\phi(J(\mathbb{Q}_p)) \rightarrow 0.$$

Proof. This is a special case of [15], Proposition 2.6. \square

Theorem 3.3.5 *The Selmer groups of the Richelot isogenies on the Jacobians of the curves $y^2 = -6f(x)$ and $y^2 = 6g(x)$ are isomorphic to $(\mathbb{Z}/2)^3$.*

Proof. Let the Jacobians of C_{-6} and C'_6 be denoted J and J' respectively. The Selmer groups of J and J' will be calculated together, because there is no obvious way to determine the size of $J(\mathbb{Q}_p)/\phi'(J'(\mathbb{Q}_p))$ without computing the size of $J'(\mathbb{Q}_p)/\phi(J(\mathbb{Q}_p))$ at the same time. We will compute them using Proposition 3.3.4.

The primes of bad reduction of both C_{-6} and C'_6 are 2, 3, 5. Using [15], Propositions 2.4 and 2.5, we can calculate the order of $J'(\mathbb{Q}_p)/2J'(\mathbb{Q}_p)$, the third nonzero term in the exact sequence of Proposition 3.3.4: it is 16 for $p = 2$, while it is 4 for $p = 3, 5$ and 2 for $p = \infty$. It is easy to calculate that the first term of the exact sequence in Proposition 3.3.4 has order 4 for $p = 2, 3, 5$ and 2 for $p = \infty$. For both curves the 2-torsion points map to $(10, 2)$, $(2, -2)$, and their product $(5, -1)$ in Sel_{ϕ} and Sel'_{ϕ} under $\delta_{\phi, C}$ and $\delta_{\phi', C'}$ respectively. The sum of the dimensions of the second and fourth nonzero terms in the exact sequence must be equal to the sum of the dimensions of the first and third nonzero terms. For $p \in \{3, 5, \infty\}$, the sum of the dimensions of the images of the subgroups generated by the 2-torsion is already equal to the sum of the dimensions of

the first and third nonzero terms, so for these p the images of the 2-torsion points generate the local image. However, for $p = 2$, we need to find two additional generators.

We check that there is a $\mathbb{Q}_2(\sqrt{6})$ -rational point on C_{-6} with x -coordinate $3 + \sqrt{6}$ whose image under δ_R is $(10, -2)$. Also, there is a $\mathbb{Q}_2(\sqrt{6})$ -rational point on C'_6 with x -coordinate $5 + \sqrt{6}$ whose image is $(10, -2)$. These new generators are independent of the image of the 2-torsion points of C_{-6} and C'_6 respectively, so we have found the full Selmer group of the isogeny for both C and C' .

p	C	C'
2	$(5, 1), (2, 2), (1, -1)$	$(5, 1), (2, 2), (1, -1)$
3	$(1, -1), (-1, 1)$	$(1, -1), (-1, 1)$
5	$(5, 1), (2, 2)$	$(5, 1), (2, 2)$
∞	$(1, -1)$	$(1, -1)$

It is now straightforward to see that the Selmer groups in both cases are generated by $(5, 1), (2, 2), (1, -1)$. \square

It follows immediately that the Selmer groups contain $(1, -1)$, which is not in the image of the 2-torsion. We can now show that $(1, -1)$ is in the Tate-Shafarevich group of the Richelot isogeny, from which it will follow that the elements of III found in Theorem 3.2.1 and Theorem 3.3.1 are not in the kernel of the map induced by the Richelot isogeny for $n = 1$.

Theorem 3.3.6 *The element of $\text{III}(\text{Jac}(C_{-6}))$ described in Theorem 3.2.1 is not in the kernel of the map on Tate-Shafarevich groups induced by the Richelot isogeny, and similarly for C'_6 .*

Proof. We will do this only for C , the calculations for C' being essentially identical. We will first represent that element as an explicit cocycle with values in $\text{Jac}(C_{-6})[2]$, apply ϕ , and show that the image is the nontrivial element $(1, -1)$ in $\text{Sel}_{\phi'}$.

Recall (Definition 3.1.13) that we write δ_i for the components of the image of δ that gives the nontrivial element of $\text{III}(\text{Jac}(C_{-6n}))$ under a fixed isomorphism $A_f \otimes \bar{\mathbb{Q}} \rightarrow \oplus_1^6 \bar{\mathbb{Q}}$ in which $\bar{\mathbb{Q}}[X]/(f_j)$ corresponds to components $2j - 1$ and $2j$. Given $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, write s for the permutation of $\{1, 2, \dots, 6\}$ induced by σ on the δ_j . By remarks in the proof of [15], Proposition 2.2 and in [15], section 2.5, we can write the element of III as a cocycle with values in $\mu_2(A_f \otimes \bar{\mathbb{Q}})/\pm 1$. As in the discussion preceding Lemma 2.1.10, we identify $A_f \otimes \bar{\mathbb{Q}}$ with $\oplus_1^6 \bar{\mathbb{Q}}$ with Galois acting by ${}^\sigma(a_1, \dots, a_6) = ({}^\sigma a_{s^{-1}(1)}, \dots, {}^\sigma a_{s^{-1}(6)})$. Indeed, the cocycle corresponding to the element of III constructed in Theorem 3.3.1 is the one that takes $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to ${}^\sigma \alpha / \alpha$, where

$$\alpha = \left(\sqrt{(\delta_1 \delta_j)} \right)_{j=1}^6 = \sqrt{(1, 1, -3(1 + \sqrt{2}), -3(1 - \sqrt{2}), 3(1 + \sqrt{5})/2, 3(1 - \sqrt{5})/2)}.$$

In particular, this cocycle, which we will denote z_α , factors through $\text{Gal}(F/\mathbb{Q})$, where F is as in Theorem 3.2.1.

Now let us write z_α as a cocycle with values in $J[2]$. Following the description in [15], section 2.5, we see that $(r_i) \in \mu_2(L')/\pm 1$ corresponds to a 2-torsion point T on the Jacobian such that $e(T, (\delta_j, 0) - (\delta_1, 0)) = r_j$ for all j from 1 to 6, where e is the Weil pairing. The rational 2-torsion divisors are 0 and $(\delta_{2k}, 0) - (\delta_{2k-1}, 0)$ for $k = 1, 2, 3$. Since two 2-torsion divisors of the form $(\delta_i, 0) - (\delta_j, 0)$ have Weil pairing 1 or -1 depending on whether the number of points appearing in both counted with multiplicity is even or odd, the rational 2-torsion points arise only from the following sequences of square roots of 1:

$$(1, 1, 1, 1, 1, 1), \quad (1, 1, -1, -1, 1, 1), \quad (1, 1, 1, 1, -1, -1), \quad (1, 1, -1, -1, -1, -1).$$

We claim that the image of $z_\alpha(\sigma)$ under the pairing with the points $(\delta_j, 0) - (\delta_1, 0)$ is one of these sequences corresponding to an element of the kernel of the Richelot isogeny if and only if σ fixes a square root i of -1 . Indeed, it is clear that the first two components of $z_\alpha(\sigma)$ are always 1, while the product of components 3 and 4 is 1 if and only if σ fixes a square root of $\delta_3 \delta_4 = -9$, and similarly for components 5 and 6.

These points are the kernel of the Richelot isogeny, which therefore maps z_α to a cocycle that factors through $\mathbb{Q}(i)$ and takes the nontrivial element of this Galois group to the rational 2-torsion point arising from the factor g_1 . This corresponds to the element $(1, -1)$ of the Selmer group of ϕ' . To see this, note that $(1, i)$ is a square root of $(1, -1)$, and the action of σ multiplies $(1, i)$ by $(1, 1)$ if σ fixes i and by $(1, -1)$ otherwise. But the image of the 2-torsion point coming from g_1 under the ϕ' -Weil pairing is $(1, -1)$, because the pullback of this point pairs trivially with the point coming from the factor f_1 on J and nontrivially with the point coming from f_2 . As a result, the image of z_α under the Richelot isogeny corresponds to the cocycle $\sigma \rightarrow {}^\sigma(1, i)/(1, i)$.

Recall from Definition 3.2.2 and Proposition 3.2.3 that the full 2-descent map $\Delta_{C'}$ is a map from $\text{Jac}(C')(\mathbb{Q})$ to $\mathbb{Q}[X]/(g)$. Composing $\Delta_{C'}$ with an isomorphism from $\mathbb{Q}[X]/(g)$ to $\oplus_{i=1}^3 \mathbb{Q}[X]/(g_i)$ obtained from the Chinese Remainder Theorem, we see that the map takes a point (x_0, y_0) to $(x_0 - \rho_i)_{i=1}^3$; in other words, its components are defined by the functions $x - \rho_i$. We remark that $g_1 = N(x - \rho_1)$ and $g_2 = N(x - \rho_2)$. It follows that if P is a point of $\text{Jac}(C'_6)$, then the image of P under $\delta_{R, C'}$, the descent map for the Richelot isogeny, is the norm of the first two components of its image under $\Delta_{C'}$.

However, using MAGMA's `TwoSelmerGroup` command to compute the fake Selmer group, it is easy to verify that the norm map from the fake Selmer group for full 2-descent to the Selmer group of the Richelot isogeny is an isomorphism for C'_6 . It follows that the image of an element of $\text{III}(C'_6)$ cannot be the image of a rational divisor, so $(1, -1)$ belongs to the Tate-Shafarevich group of the Richelot isogeny on C'_6 . \square

Remark 3.3.7 This proof applies to any twist C'_{6n} , where n is a product of elements of the set S described in Theorem 3.3.1, for which we know that no rational point on the Jacobian of C'_{6n} maps by δ_R to $(1, -1)$. However, there is no reason to expect this to be true in general; if the rank is large, it is very unlikely that the fake Selmer group for multiplication by 2 would be isomorphic to the Selmer group of the Richelot isogeny, and the proof would fail.

References

- [1] W. Barth, C. Peters, and A. van de Ven, *Compact Complex Surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete, **3**. Folge, Band **4**, Springer-Verlag, 1984.
- [2] E. Bombieri and D. Mumford, *Enriques' classification of surfaces in char. p , II*, Complex Analysis and Algebraic Geometry – Collection of papers dedicated to K. Kodaira, ed. W.L. Baily and T. Shioda, Iwanami and Cambridge Univ. Press (1977), 23–42.
- [3] M. Bright, *Brauer Groups of Diagonal Quartic Surfaces*, J. Symbolic Computation, to appear.
- [4] M. Bright, *Computations on Diagonal Quartic Surfaces*, Unpublished PhD dissertation, Cambridge University, 2002, available at www.boojum.org.uk.
- [5] M. Bright and H. P. F. Swinnerton-Dyer, *Computing the Brauer-Manin obstructions*, Math. Proc. Camb. Phil. Soc. **137** (2004), 1–16.
- [6] N. Bruin and E. V. Flynn, *Exhibiting SHA[2] on hyperelliptic Jacobians*, To appear in J. Number Theory.
- [7] Cassels and Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, LMS Lecture Notes **230**, Cambridge University Press (1996).
- [8] P. Deligne, Cohomologie des intersections complètes, Exposé XI in *Groupes de monodromie en géométrie algébrique (SGA 7 II)*, Lecture Notes in Math. **340**, Springer, Berlin, 1973.
- [9] R. Hartshorne, *Algebraic Geometry*, GTM **52**, Springer-Verlag, New-York, 1977.
- [10] R. Hartshorne, *Equivalence relations of algebraic cycles and subvarieties of small codimension*, Algebraic Geometry, Arcata 1974, Amer. Math. Soc. Proc. Symp. Pure Math. **29** (1975), 129–164.
- [11] Yu. Manin, *Cubic forms: algebra, geometry, arithmetic*, North-Holland Mathematical Library **4**, North-Holland, Amsterdam, 1986 (2nd edition, translated by M. Hazewinkel).
- [12] J. S. Milne, *Étale Cohomology*, Princeton Mathematical Series **33**, Princeton University Press, Princeton, 1980.
- [13] D.R. Morrison, *On K3 surfaces with large Picard number*, Invent. Math. **75** (1984), 105–121.
- [14] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149.
- [15] E.F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), 447–471.
- [16] J.-P. Serre, *Local Fields*, GTM **67**, Springer-Verlag, New-York, 1979.
- [17] T. Shioda, *Algebraic cycles on certain K3 surfaces in characteristic p* , Manifolds–Tokyo 1973 (Proc. Internat. Conf., Tokyo, 1973), Univ. Tokyo Press, Tokyo (1975), 357–364.
- [18] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277.
- [19] R. van Luijk, *An elliptic K3 surface associated to Heron triangles*, Journal of Number Theory, bf 123 (2007), 92–119.
- [20] R. van Luijk, *K3 surfaces with Picard number one and infinitely many rational points*, preprint, available at [arXiv:math.AG/0506416](https://arxiv.org/abs/math/0506416) (2005).
- [21] *Various implementations used for this paper*, available from the authors upon request.